Governance, Risk, and Best Value Committee

10.00am, Tuesday, 11 October 2022

Internal Audit Update Report: 1 May to 31 August 2022

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

1. Recommendations

1.1 It is recommended that the Committee:

1.1.1. reviews the outcomes of the final 'red' audits and those with high rated findings supporting the 2021/22 Internal Audit (IA) annual opinion presented to Committee in August 2022;

1.1.2. notes improvement recommendations in relation to annual planning made by the Chartered Institute of Internal Auditors as part of the five-yearly External Quality Assessment of the Council's IA function;

1.1.3. approves proposed revisions to 2022/23 IA annual plan;

1.1.4. notes progress with delivery of the 2022/23 IA annual plan;

1.1.5. notes the current IA risk profile; and

1.1.6. notes progress with delivery of IA key priorities and ongoing areas of focus.

Laura Calder
Senior Audit Manager

Legal and Assurance, Corporate Services Directorate

E-mail: laura.calder@edinburgh.gov.uk | Tel: 0131 469 3077

Report

Internal Audit Update Report: 1 May to 31 August 2022

2. Executive Summary

2.1 The IA annual opinion for 2021/22 was presented to Committee on 23 August 2022. The remaining reports which support the 2021/22 annual assessment have now been finalised. All reports with either an overall red (Significant Improvement Required) outcome or include any red (High) rated findings are presented to the Committee for scrutiny.

2.2 The Chartered Institute of Internal Auditors (IIA) identified areas for improvement during their five-yearly External Quality Assessment (EQA) of the Council's IA function in relation to annual plan delivery and aligning resources and capacity to key risks and controls. As a result, changes to the 2022/23 IA annual plan are proposed for Committee approval.

2.3 Progress continues with delivery of the 2022/23 IA annual plan, with 26 of 40 audits (65%) included in the proposed re-based plan in progress. This includes 24 of the 31 (77%) of the audits to be completed across the Council.

2.4 Timeframes have been agreed with the Corporate Leadership Team (CLT) and Directorates for delivery of the remainder of the proposed re-based 2022/23 IA annual plan to support delivery throughout the remainder of the year.

2.5 The specification for a replacement IA system has been finalised, and procurement for this is underway.

2.6 The majority of IA risks are currently being managed within risk appetite, with appropriate actions agreed to mitigate current risks that are outwith appetite.

3. Background

2021/22 Internal Audit Annual Plan

3.1 The IA annual opinion for 2021/22 was presented to Committee on 23 August 2022. The remaining reports which support the 2021/22 annual assessment have now been finalised.

3.2 All reports with either an overall red (Significant Improvement Required) outcome or include any red (High) rated findings are presented to the Committee for scrutiny. A total of seven reports are presented to Committee for scrutiny and opportunity

provided to discuss findings raised with the relevant service area and IA, where relevant.

3.3 Elected Members may also request presentation of other reports that do not meet these criteria at Committee. A total of 16 further reports are available and have been provided to members to review via the GRBV MS Teams room (see Appendix 1 for details).

External Quality Assessment (EQA)

3.4 An EQA of the City of Edinburgh Council's IA function was undertaken by the Chartered Institute of Internal Auditors (IIA) during 2021/22 in line with Public Internal Audit Standards (PSIAS). A copy of this report is presented to Committee on today's meeting agenda at item 8.1.

2022/23 Internal Audit Annual Plan

3.5 The Committee approved the 2022/23 IA annual plan in March 2022 which aimed to deliver a total of 45 audits (38 across the Council and 7 for ALEOs). In addition, the 2021/22 IA annual opinion advised that 6 audits remaining from the 2021/22 IA annual plan would be carried forward to the 2022/23 plan taking the total number of audits due for completion in 2022/23 to 51.

Internal Audit reports for other organisations included within the IA annual plan

3.6 All audits performed for the Lothian Pension Fund (LPF) are subject to separate scrutiny by the Pensions Audit Sub-Committee and the Pensions Committee. Progress with delivery of these audits is included in this paper for completeness.

3.7 Similarly, audits performed for the Edinburgh Integration Joint Board (EIJB) are presented to the EIJB Audit and Assurance Committee for scrutiny, with any reports that are relevant to the Council being subsequently referred to the GRBV Committee.

3.8 Audits performed for the Council that are relevant to the EIJB will be recommended for referral to the EIJB Audit and Assurance Committee by the GRBV Committee.

3.9 All audits performed for other Arms-Length External Organisations (ALEOs) are reported to the relevant management teams and audit and risk committees of those organisations as appropriate.

4. Main report

Remaining 2021/22 audit reports for scrutiny

4.1 The following seven audit reports assessed as 'significant improvement required' or with 'high' rated findings which support the IA annual opinion presented to Committee in August 2022 have been finalised and are provided to members for scrutiny:

Audit Title	Overall Audit Assessment	Number of findings raised		
		H	M	L
1. Housing Property Services Repairs Management During Covid-19	Some Improvement Required	1	1	3
2. Implementation of historic whistleblowing recommendations	Some Improvement Required	1	-	1
3. Payment Card Industry Data Security Standard Compliance	Significant Improvement Required	1	3	-
4. Planning and Performance Framework Design Review	Some Improvement Required	1	1	1
5. Parking and Traffic Regulation	Significant Improvement Required	3	1	-
6. Technology Vulnerability Management	Significant Improvement Required	1	2	-
7. Fraud and Serious Organised Crime	Significant Improvement Required	1	1	-

4.2 Copies of the following reports together with an update from management are provided as part of today's meeting agenda:

- Housing Property Services Repairs Management During Covid-19 (item 8.3.1)
- Parking and Traffic Regulation (item 8.3.2)

4.3 A total of 16 further reports that have been assessed as either 'some improvement required' or 'effective' and have no high rated findings are available and have been provided to members to review via the GRBV MS Teams room.

4.4 A list of the 16 audit reports and outcomes is provided in Appendix 1. Members have requested that the following four reports are presented for scrutiny and that relevant Council officers are available to respond to any questions:

- Employee wellbeing (Some Improvement Required)
- CGI Performance Reporting (Some Improvement Required)
- Management and Allocation of Covid-19 Grant Funding (Effective)

4.5 The following report is a legally privileged and confidential report, and therefore will be considered in private at item 8.3.3:

- Health and Safety - Implementation of Asbestos Recommendations (Some Improvement Required)

IA External Quality Assessment (EQA)

4.6 The EQA finalised in September 2022 concluded that the Council's IA function is generally conforming with the PSIAS. Two recommendations to address partial conformance with the standards were made by the IIA.

4.7 One of these recommendations was related to audit planning and reviewing the audit plan to ensure a risk-based and proportionate approach which focuses more on the Council's strategic risks, core governance and control areas and is aligned to priorities and available resources.

4.8 As noted above copy of the full EQA report is available in the agenda for today's meeting at item 8.1.

IA capacity, EQA recommendations and impact on 2022/23 Annual Plan

4.9 The 2022/23 IA annual plan approved by Committee in March 2022 included a total of 45 audits (38 across the Council and 7 for ALEOs). In addition, 6 further audits from the 2021/22 IA annual plan that were not completed were carried forward to bringing the total number of audits for 2022/23 to 51. Two audits related to Covid-19 were consolidated leaving a total of 50 audits to be delivered in 2022/23.

4.10 Of the 50 audits, 11 specialist audits were due to be delivered by co-source partners (PwC;10 and NHS Lothian;1), with the remaining 39 audits to be delivered by the Council's IA team.

4.11 The structure of the IA function includes 12 full-time equivalent (FTE) posts. Due to a number of ongoing capacity challenges, including a vacant Chief Internal Auditor post; long term absence at manager level; maternity leave and a number of acting-up arrangements to support vacant posts, the current FTE is 8. As a result, capacity to deliver the plan as agreed by Committee in March 2022 is significantly reduced.

4.12 In addition, the EQA report completed by the IIA noted that for the past 4 years, IA has struggled to deliver the annual plan, and that failure to complete the annual audit programme within the financial year (without use of additional co-source resource over and above the planned co-source requirement at significant additional budget) is a weakness which should be addressed.

4.13 The IIA review has suggested that a significant change is needed in the way the plan is designed and delivered to avoid annual re-occurrence of the same challenge. The IIA recommend a move away from a five-year cyclical programme which aims to cover the whole organisation to an audit plan which provides assurance on business-critical risks and core controls whilst considering the context and challenges of the public sector environment of the Council.

4.14 They further recommend that the audit plan is reviewed regularly to ensure the focus remains on business-critical risks and priorities, and where relevant, proposals should include an option for delivering an internal audit opinion only in relation to the work completed (i.e., limited in scope).

4.15 As a result of internal capacity challenges and the EQA recommendations, the Council's IA function has engaged with directorates and services to develop a rebased 2022/23 IA plan which focuses on key risks and controls and reflects actual IA FTE and capacity while limiting the use of external co-source resource to reviews of specialist areas only.

Proposed re-based 2022/23 IA annual plan

4.16 Following review of IA methodology and capacity for the remainder of 2022/23, IA has engaged with directorates to develop a re-based annual plan which focuses on key risks and priorities and results in a proposed net reduction of 10 audits.

4.17 The re-based IA plan proposes that 7 audits are removed as they are no longer required and/or linked to Council's strategic risks, core governance and control areas. A further 10 audits in the originally approved 2022/23 IA plan have been proposed for consideration as part of 2023/24 planning, enabling alignment of priorities with available resources both within services and IA.

4.18 Following engagement with services, 5 new audits of new and emerging priorities are proposed for inclusion within the re-based 2022/23 IA plan.

4.19 In addition, the number of audits included in the LPF 2022/23 annual plan has been increased from 2 to 4. These specialist audits will be completed by PwC with oversight from the Council's IA management team.

4.20 As a result of the changes outlined above, the total number of audits being delivered in the proposed rebased 2022/23 annual plan is 40, with 31 completed across the Council and 9 for ALEOs. 29 audits will be delivered by the Council's IA team. Details and rationale are provided at Appendix 2.

4.21 The number of audits proposed for completion across the Council in 2022/23 (31) is aligned to previous years (31 audits in 2021/22; 34 audits in 2020/21 and 32 audits in 2019/20).

4.22 Financial impacts associated with delivery of the 2022/23 IA annual plan are set out at section 6 of this report.

4.23 It is considered that completion of the proposed rebased plan will provide sufficient assurance of the Council's governance; risk and control frameworks to support provision of an annual audit opinion, with the aim of completing audits no later than 30 April 2023, to enable the 2023/24 IA plan to commence in a timely manner.

Delivery progress of the proposed re-based 2022/23 IA annual plan

4.24 Of the 40 audits proposed for completion:

- 4 draft reports are with management for response;
- 3 draft reports are currently being prepared by IA;
- 8 further audits are in fieldwork;
- 11 audits are currently being planned; and
- 14 are not yet started.

4.25 The 26 audits in progress include 24 of the 31 (77%) of the audits to be delivered across the Council, including two ongoing 'agile' major project reviews.

4.26 Of the 14 audits not yet started, 5 are specialist audits that will be delivered by PwC/NHS Lothian. Timescales for all audits have been agreed with services and co-source partners.

4.27 Further detail on the content and delivery timescales for the re-based 2022/23 IA plan is included at Appendix 3.

4.28 To further support timely completion of the re-based plan, scoping of audit work will be reviewed to ensure a focus on key risks and controls only and alignment with allocated budgets. Where appropriate design only or lighter touch focused reviews will be completed. This is in alignment with recommendations made by the IIA as part of the EQA.

IA Risk Profile

4.29 The IA risk register continues to highlight that IA's most significant current risks that currently exceed target risk appetite are:

- Capacity – IA capacity is currently below the FTE required to deliver the IA plan originally approved without use of additional resource at significant cost.
- Assurance – risk that current audit plan is not aligned to business-critical risks and controls and that reliance on a five cyclical programme may result in disproportionate assurance on areas considered lower risk by management.
- Applications and systems design – support for the current IA system has been extended to December 2026 which removes the immediate need for replacement, however, associated procurement compliance risks, and system-based efficiencies which would support IA capacity challenges should be considered.
- Budget Management and Best Value – system procurement costs; and PwC support for delivery of specialist audit and/or additional generalist reviews.

4.30 Appropriate actions are currently being mitigated to address these risks including proposals within this report.

Progress with Internal Audit key priorities

4.31 Progress with IA key priorities and ongoing areas of focus is detailed below:

- Implementation of recommendations and continuous improvement actions identified in the recently completed EQA.
- Implementation of a new risk-based approach to follow-up and validating agreed audit actions.
- A refresh of audit reporting including redesign of audit reports to focus on key messages, and a review of CLT/Committee reporting to support decision making and scrutiny.
- Revision of the IA methodology including the scoping approach for audits and terms of reference to ensure a streamlined approach focused on key risks and controls.
- Refreshed IA intranet (Orb) pages are available, together with development of controls training for employees which will be available via the Council's myLearning Hub platform.

- Work to procure a replacement IA system is progressing with support from Commercial and Procurement Services.

5. Next Steps

5.1 IA will continue to monitor progress with plan delivery and the other activities noted in this report.

6. Financial impacts

6.1 The re-based plan would result in a reduction of budgeted costs associated for audits due to be completed by external co-source partners (PwC), with costs for 3 audits carried forward aligned to the 2021/22 budget; and the 2 additional LPF audits directly recharged. In addition, 1 audit initially proposed for PwC completion will be completed in-house as relevant experience of the audit area is available within the IA team.

6.2 Delivery of the 16 audits removed from the original 2022/23 plan would require additional resource which is unlikely to be filled internally within sufficient timescales, therefore reliance would be placed on external co-source resources with an estimated cost of circa £15k per audit (total £250k) which would need to be approved by the Finance and Resources Committee.

6.3 There are no associated budget implications for completion of audits completed for ALEOs as direct recharge is applied for costs incurred.

6.4 Procurement of a replacement IA system will incur additional costs that have not yet been fully quantified.

7. Stakeholder/Community Impact

7.1 Delivery of an audit plan which is not aligned to key risks and priorities will result in a disproportionate use of limited resources across both services and IA.

7.2 In addition, failure to take account of best practice and IIA recommendations in relation to audit planning and engagement may result in reputational damage to the Council.

8. Background reading/external references

8.1 Process for approving changes to the Internal Audit annual plan – August 2018 – item 7.9

8.2 Public Sector Internal Audit Standards

8.3 Approved IA 2022/23 annual plan March 2022 - item 8.4

8.4 The Chartered Institute of Internal Auditors: External Quality Assessment Report (see item 8.1 on today's meeting agenda).

9. Appendices

9.1 Appendix 1- 2021/22 Audits assessed as either ‘some improvement required’ or ‘effective’ with no high rated findings

9.2 Appendix 2 – Summary of proposed 2022/23 IA Annual Plan Changes

9.3 Appendix 3 - Rebased 2022/23 IA Plan, Delivery Progress and Expected Completion

Appendix 1 – 2021/22 Audits assessed as either 'some improvement required' or 'effective' with no high rated findings

Audit Title	Overall Audit Assessment	Number of findings raised		
		H	M	L
1. Health and Safety - Implementation of asbestos recommendations	Some Improvement Required	-	3	2
2. Complaints Management	Some Improvement Required	-	2	1
3. Employee Wellbeing	Some Improvement Required	-	3	-
4. Management and Allocation of Covid-19 Grant Funding	Effective	-	1	-
5. Implementation of Child Protection Recommendations	Effective	-	1	1
6. CGI performance reporting	Some Improvement Required	-	2	1
7. Employee Lifecycle Data & Compensation and Benefits Processes	Effective	-	-	1
8. Verint system	Effective	-	-	-
9. Capital Budget Setting and Management	Effective	-	1	1
10. Digital and Smart City Strategy	Effective	-	-	2
11. Council Tax and Non-Domestic Rates	Some Improvement Required	-	2	2
12. Criminal Justice Social Work – Community Payback Orders	Effective	-	1	-
13. Transformation and Benefits Realisation	Effective	-	2	-
14. Health and Social Care Partnership Volunteer Support Arrangements	Effective	-	-	-
15. Householder Planning Applications and use of Uniform System	Some Improvement Required	-	2	-
16. The Management of Development Funding	Effective	-	-	1

Appendix 2 – Summary of proposed 2022/23 IA Annual Plan Changes

		Council	ALEOs	Total
Total Audits per 2022/23 Annual Plan including 2021/22 carry forward* **Further Covid-19 lessons learned 21/22 and 22/23 reviews consolidated*		**43***	**7**	**50**
Less:				
Audits proposed for removal	**Rationale**	**7**	**-**	**7**
1) Quality Improvement and Curriculum	Second line assurance provided by Education Scotland			
2) Management of Waiting Lists and Assessments	Risks will be considered as part of 2023/24 audit plan in alignment with National Care Service proposals; transition and preparation.			
3) Partnership Financial Sustainability				
4) Oversight of Care homes				
5) Physical Security (Operational Properties)	Initial risk assessment was linked to compliance with Covid-19 guidance which is no longer applicable, area was previously audited in 2021			
6) Business Support Arrangements	Linked to business plan and workforce review will be considered as part of 2023/24 workforce planning audit			
7) Implementation of Covid-19 lessons learned	Two previous audits done in this area in 2020/21 and 2021/22 - is now considered business as usual			
Audits to be considered in 2023/24	**Rationale**	**10**	**-**	**10**
1) Transfer of the Management of Development Funds Grant	Scottish Government have confirmed now only required every 2 years as low risk			
2) Fleet Operations	Ongoing restructure in area – work to be considered 2023/24			
3) Refugee and Migration Services	Area of priority but current capacity issues due to ongoing Ukraine support			
4) Schools Attendance	Lighter touch review to be considered in 2023/24			
5) Health and Safety - Public Safety (PwC)	Initial assessment linked to Covid-19 but value in considering in 2023/24 due to redesign and restructure			
6) Progress with Implementation of the Governance and Assurance Model	Timing to be realigned with completion of framework design and review of process in operation			

7) Workforce Capacity to Support Service Delivery	Timing to be aligned with review of Business Plan and priorities and development of medium term business plan			
8) Food and Water Testing	Priority area to be considered early in 2023/24			
9) Council House Allocations	Priority area to be considered early in 2023/24			
10) Community Centres	Initial risk assessment linked to Covid-19 guidance which is no longer applicable. Organisational review ongoing in the area. This is scheduled to conclude late 2022 before a period of matching and assignment takes place. Directorate review of community centres is ongoing and this will be reported to committee as early as possible in 2023. An audit with refreshed focus which will provide assurance on key risk areas following the conclusion of the current review (early 23/24).			
Add				
Audit title	**Rationale**	**5**	**2**	**7**
1) Levelling Up Fund - Granton Gas Holder	Requirement inline with grant funding award			
2) City Deal Integrated Employer Engagement	Audit programme is a requirement of funding award			
3) Vendor fraud review	Service area request in response to internal review			
4) Schools Admissions (Follow- up)	Lighter touch audit - Service area request in response to priorities			
5) Health and Social Care – Total Mobile Project Implementation	Service area request to identify lessons learned to support similar projects in future			
6) LPF – Third party supplier management	LPF request to support ongoing priorities			
7) LPF – Information Governance				
Total Audits to be Delivered in 2022/23		**31**	**9**	**40**
Audits to Be Delivered by PwC / NHS Lothian (for EIJB)		**6**	**5**	**11**
Audits to be Delivered by the Council		**25**	**4**	**29**

Appendix 3 – Rebased 2022/23 IA Plan, Delivery Progress and Expected Completion

Audits at reporting stage			Expected Completion
1.	Corporate Services	**Implementation of the New Consultation Policy** Review of implementation and application of the Council's new consultation policy and supporting processes.	October 2022
2.		**Council Emissions Reduction Plan (CERP)** Review of the framework designed to support implementation of the Council Emissions Reduction Plan.	
3.		**Vendor Bank Mandate Process** Review of the design and effectiveness of processes established to verify and process requests to change vendor bank details on Oracle, the Council's financial management system.	
4.	Council Wide	**Records Management and Statutory Requests** Review of the design and effectiveness of processes implemented to support effective records management and compliance with statutory request requirements.	
5.		**Allocation and Management of Purchase Cards** Review of the allocation, management, use and monitoring of purchase cards across the Council.	
6.	Place	**Port Facility Security Plan** Annual review of existence and operation of the Port Facility Security Plan as per Department for Transport requirements.	
7.	Council Wide	**Induction, Essential Learning, and Training for Officers and Elected Members** Review of established induction; essential learning, and ongoing training delivered across the Council for both officers and elected members.	
Total audits at reporting stage			**7**
Audits in progress (fieldwork)			**Expected Completion**
8.	Corporate Services	**Enterprise Resource Planning (ERP)** Ongoing agile review of the project management and governance arrangements supporting implementation of the enterprise resource planning system.	Ongoing agile audit
9.	Place	**Tram to Newhaven** Ongoing agile review of project governance; procurement; and gateway decisioning and payments. The audit will include ongoing assessment of the ongoing controls supporting the funding model.	
10.	Education and Children's Service	**Availability of Early Years Education and Alignment with the Poverty Strategy** Review of the strategy to support expansion of the early years education programme and its alignment with the Council's poverty strategy. Review will also consider the design and effectiveness of processes to established to	

		support allocation of places in line with eligibility criteria, and the Council's oversight of early years private partner providers.	
11.	Place	**Active Travel Project Management and Delivery** Review of the design and operating effectiveness of the key controls supporting management; governance; and delivery of the Active Travel programme.	November 2022
12.	Corporate Services	**Security Operations Centre (PWC)** Review of the adequacy and effectiveness of contractual security services delivered through the established CGI Security Operations Centre to the Council**.**	
13.	Place	**Repairs and Maintenance Framework (Operational Properties)** Review of the design and effectiveness of the new repairs and maintenance framework for Council operational properties prior to implementation.	
14.	Council Wide	**Application technology controls - SEEMiS and SWIFT** Review of the general (change management and access) and application (transaction processing) controls applied to technology applications hosted on Council networks and used to support service delivery.	
15.		**Validation of Implementation of Previously Closed Management Actions** Review of a sample of previously implemented and closed IA agreed management actions to confirm that they have been effectively sustained.	March 2023
Total reviews in fieldwork			**8**
Audits at planning stage			**Expected Completion**
16.	Corporate Services	**Enterprise Architecture Arrangements (PWC)** Review of the adequacy and effectiveness of established Council and CGI enterprise architecture arrangements to support change implementation in line with the Council's Digital and Smart City Strategy and support consistent alignment and use of technology (where possible) across the Council.	December 2022
17.	EIJB	**Governance of Directions** Review of governance arrangements for directions to ensure they are associated with EIJB decisions; are revised in response to transformation, service redesign, and financial developments; and partner implementation and performance is monitored.	
18.	Council Wide	**Day Care to Adult Social Care Transition Arrangements** Review of the design and effectiveness of processes established to support the transition of services for young adults with a disability or complex needs (Education and Children's Services) to adult social care (Health and Social Care).	
19.		**Management of the Housing Revenue Account (Capital and Revenue)** Review of the processes established to support both the capital and revenue elements of the Housing Revenue	January 2023

		Account, and management and allocation of HRA reserves	January 2023
20.		**Preparation for IFRS 16 – Lease Accounting** Review of the Council's preparation for implementation of the new single lessee accounting model that recognises assets and liabilities for all material leases longer than 12 months, and proposed processes for accounting for any low value leases.	
21.	Corporate Services	**Risk Management – CGI and Digital Services (PWC)** Review of CGI and Digital services process supporting identification; assessment; recording; management; and escalation of relevant technology risks	
22.	Health & Social Care Partnership	**Sensory Support** Review of the commissioning and partnership / supplier management arrangements for provision of sensory support services to adults aged 16 and over.	
23.	^LPF	**Project Forth – Programme Management (PwC)**	
24.	Place	**Granton Waterfront – Levelling-up** Assurance required by the UK Government Department of Levelling Up, Housing, and Communities in relation to the conditions attached to the Granton Gas Holder LUF Grant Determination.	February 2023
25.		**City Deal Integrated Employer Engagement** Service request as part of required audit programme to support grant funding requirements.	
26.	Council Wide	**Review of Historic Disciplinary Cases and Complaints (Project Apple requirement)** Review of historic disciplinary cases and complaints to confirm whether any handled by for employees noted in Project Apple outcomes had been appropriately investigated and reported.	March 2023
Total reviews at planning stage			**7**
Audits not yet started			**Expected Completion**
27.	Place	**Health and Safety of Outdoor Infrastructure (PwC)** Review of the design of effectiveness of processes established to ensure the health and safety of outdoor infrastructure (for example walls; railings; paths; and equipment in children's public play areas) owned and managed by the Council.	December 2022
28.	Corporate Services	**Insurance Services (PwC)** Review of the adequacy of insurance arrangements across the Council, including the process applied to address any questions received from insurers, and implement any insurance provider recommendations and requirements.	January 2023
29.	Education and Children's Services	**Children's Social Work Practice Review Teams** Review of processes and procedures established to support review of children's social work practices across social work practice teams to confirm that the levels of support provided remain appropriate to meet the child's	

		needs, and that all changes in circumstances have been considered.	February 2023
30.	^EIJB	**Review of set aside budget setting and monitoring processes (NHSL)** Including identification of services and their associated costs; underlying budget assumptions; and financial reporting to the IJB on ongoing set aside budget management.	
31.	^LPF	**Information Governance (PWC)**	March 2023
32.	^LPF	**Third Party Supplier Management (PWC)**	
33.	^LPF	**Adequacy of technology security assurance arrangements (PWC)**	
34.	Education and Children's Services	**Schools Admissions – Follow-up** Service request to complete focused follow-up of audit previously completed in 2019/20 including issues with the Seemis system.	March 2023
35.	Council Wide	**Self-Directed Support – Children and Adult Social Care Services** Review of the adequacy and effectiveness of established self-directed support arrangements, including compliance with the Scottish Government's framework of standards, and consistency of application across localities.	
36.		**Empowered Learning Programme** Review of the Empowered Learning programme which underpins Digital Learning across all aspects of Learning and Teaching extending from our Early Years through primary, secondary and special needs sectors.	
37.	Health and Social Care	**Implementation of Total Mobile** Review of implementation of Total Mobile project to identify lessons learned and improvement actions to support implementation of similar projects in future.	
38.	^Tattoo	To be confirmed in line with key risks and priorities	March 2023
39.	^SEStran	To be confirmed in line with key risks and priorities	
40.	^LVJB	To be confirmed in line with key risks and priorities	
Total reviews not yet started			**14**

^Audits completed for Arm's Length External Organisations

Internal Audit Report

Implementation of Historic Whistleblowing Recommendations

12 July 2022

CW2106

Overall Assessment	**Some improvement required**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Some improvement required

Overall opinion and summary of findings

Whilst processes for coordinating and reporting on whistleblowing investigation outcomes are generally operating effectively, we identified some minor weaknesses in the design and operating effectiveness of the supporting control framework operated by the Governance Team.

In addition, we identified some significant weaknesses in the design and operating effectiveness of directorate level controls for monitoring and evidencing progress and implementation of whistleblowing recommendations.

Consequently, one Low rated and one High rated finding has been raised.

The Low rated finding highlights opportunities to improve the content of the whistleblowing policy and to enhance the supporting second line operational processes to ensure:

- formalisation of roles and responsibilities;
- SMART recommendations are made;
- reports provided to committees are fully complete and accurate; and
- the Council's online records retention schedule is updated to reflect established arrangements for whistleblowing disclosures.

The High rated finding highlights the need for all directorates to establish consistent processes to ensure there is adequate oversight of whistleblowing action implementation progress and reporting in line with the previously agreed actions arising from the "Implementation of Assurance Actions and Linkage to Annual Governance Statements" audit completed in July 2020.

Specific improvements are required to ensure that:

- action owners and target dates are identified for whistleblowing management actions at the outset and appropriate handover processes are in place where action owners leave their roles;
- implementation progress is monitored by directorates to ensure actions are fully complete within agreed timescales, with regular updates provided to the whistleblowing team where appropriate;
- evidence to support implementation is retained centrally within directorates and securely for an appropriate period;
- consistent and accurate reporting of actions plans to senior officers and Committee including providing updated where actions are incomplete or delayed in line with previously reported timescales; and
- reporting arrangements are reviewed to ensure that where a previously agreed and reported action is deemed to be inappropriate or no longer applicable the service, these are reported to Committee to ensure transparent Committee review and oversight.

Implementation of these recommendations, together with the recommendations raised in the Tanner review, should support consistent achievement of the Council's objectives to ensure that recommendations raised in historic whistleblowing cases have been effectively implemented and sustained.

Alignment with the December 2021 Culture Review

Our work commenced in August 2021, prior to publication of the Independent Review of Whistleblowing and Organisational Culture report by Susanne Tanner in December 2021, and included review of a sample of

whistleblowing recommendations. In addition to the findings included in this report our review highlighted a number of themes that are aligned with the recommendations included in the December 2021 report and actions detailed in the Council's approved implementation plan.

To minimise duplication, no audit recommendations on these areas are included in this report, however the outcomes of our work have been mapped to the relevant Tanner report recommendations and the Council's implementation plan. Further detail has been shared with the Inquiry and Review Programme Manager for consideration when progressing similar agreed actions within the Tanner report.

Audit Assessment

Audit Areas	Findings	Priority Rating	Areas of good practice
• Whistleblowing - Legal and Assurance	1. Corporate Whistleblowing policy and procedures 2. Directorate Whistleblowing monitoring and reporting processes	**Low**	• A central register is held by the Council's Whistleblowing Team to record all whistleblowing disclosures made and any associated recommendations arising from closed investigations. • The Whistleblowing Team communicate regularly with service areas to obtain updates on the status of whistleblowing recommendations made. • A review of thematic areas for improvement identified from a historic child protection complaint in schools confirmed a comprehensive approach has been developed to address all issues raised.
• Implementation of Whistleblowing recommendations - Directorates		**High**	

Background and Scope

The City of Edinburgh Council (the Council) must uphold the highest standard of conduct and ethics in all areas of its work. The Public Interest Disclosure Act 1998 is an amendment to the Employment Rights Act 1996 and is specifically designed to protect individuals or whistle-blowers, who disclose information in the public interest where they have concerns about any aspect of their employer's activities.

Council Whistleblowing policy and procedures

The Council's current Whistleblowing policy was introduced in May 2014. The policy was last reviewed and approved by the Council's Finance and Resources Committee in May 2019. A further review was undertaken in 2020 with a number of draft changes and improvements proposed. However, adoption of the policy was paused to enable further revision following conclusion of the Council's Independent review of Whistleblowing and Organisational Culture in December 2021.

The main way to disclose concerns is through the Council's independent and confidential whistleblowing service operated by Safecall. Disclosures can also be made directly to a Manager within the Council, who must then refer the disclosure to Safecall.

When a new disclosure is received, Safecall decide if the matter is minor/operational or major/significant (the current classifications) and will liaise with the Council to confirm investigation and reporting arrangements. This can include instructing Council Officers to complete investigations where appropriate.

Whistleblowing investigation report recommendations

Whistleblowing investigation reports detail investigation outcomes and where appropriate include recommendations to address any issues identified and are provided to relevant Council directorates to implement following scrutiny by GRBV Committee. Directorates should then allocate owners to implement the recommendations.

Quarterly and annual reports are provided to the Council's Governance, Risk and Best Value committee on whistleblowing activity and outcomes.

Recent internal audit reviews

The "Implementation of Assurance Actions and Linkage to Annual Governance Statements" audit completed in July 2020 highlighted the need for Directorates to establish frameworks to support recording, monitoring and oversight of assurance actions (including Monitoring Officer and whistleblowing actions). The related management actions were closed in August 2021 as Directorates confirmed they would implement supporting processes which would include actions arising from monitoring officer and whistleblowing reporting.

Independent Review of Whistleblowing and Organisational Culture

In October 2020, Councillors commissioned Susanne Tanner QC to undertake an independent inquiry into Whistleblowing and Organisational Culture. The review considered how the Council deals with complaints of wrongdoing, focusing on the period from May 2014, when the current Whistleblowing Policy was introduced. The outcomes of the review were presented at the full council meeting on 16 December 2021.

On 10 February 2022, the Council approved an implementation plan in response to Ms Tanner's recommendations. The plan covers a number of areas for improvement including policy development and review, the Council's approach to investigations, training and development, and systems and processes.

Scope

The objective of this review was to assess the adequacy of design and operating effectiveness of the key controls established to ensure that recommendations raised in historic whistleblowing cases have been effectively implemented and sustained.

This includes an assessment on whether the design and effectiveness of the control environment supports achievement of the following Council Business Plan objectives:

- Wellbeing and equalities – focus on child and adult support and protection.

Risks

The review will also provide assurance in relation to the following risks recorded in the CLT risk register:

- Health and Safety (including public safety)
- Governance and Decision Making
- Service Delivery
- Regulatory and Legislative Compliance
- Reputational Risk

Audit Approach

Testing was performed on major and minor whistleblowing cases closed between June 2018 and June 2021. Sampling covered all Directorates including the Edinburgh Health and Social Care Partnership, and all whistleblowing cases involving child protection which were closed between May 2014 to June 2021.

Limitations of Scope

It is acknowledged that, due to their nature, recommendations from child protection reviews often require a multi-agency response or action by an external agency. The scope of this review will be limited to processes established by the Council to implement, monitor and report on recommendations made regarding Council services.

Reporting Date

Our audit work concluded on 02 May 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Corporate Whistleblowing policy and procedures

Finding Rating	Low Priority

1. Whistleblowing policy

Review of the current Corporate Whistleblowing policy highlighted the following:

a) Chief Social Work Officer engagement - sections 4.2.13 and 4.2.14 of the current policy notes that the Whistleblowing hotline provider may determine that issues fall under the scope of other Council policies such as Child Protection and will liaise with council officers as necessary in order to progress their investigation.

The whistleblowing policy does not specifically mention the need to engage with the Chief Social Work Officer, where required, although it is noted that this happens in practice through officer referrals. The policy does include other roles that should be engaged such as the Monitoring Officer, Chief Executive and Executive Directors.

b) Implementation progress monitoring - GRBV has requested that implementation progress for recommendations arising from whistleblowing investigations is monitored, with Internal Audit reviewing a sample of completed actions on a periodic basis as part of the Internal Audit rolling cycle.

Roles and responsibilities for ensuring that whistleblowing recommendations are allocated and implemented, and ongoing implementation monitoring are not formally detailed in the current Whistleblowing policy.

Executive Director's responsibility to monitor the completion of management actions/recommendations arising from investigations and provide confirmation of closure to the Monitoring Officer is included at section 4.8.5 of the draft Whistleblowing policy (as at 2020). Publication of the revised draft was paused pending the conclusion of the Council's Independent review of Whistleblowing and Organisational Culture. However, in order to support this process, custom and practice since introduction in 2014 has been for the Whistleblowing team issue standard template emails setting out requirements for Executive Directors to notify the Whistleblowing team of a responsible officer and also when management actions have been completed.

c) Record retention - Section 10.3 of the current Whistleblowing policy states details of all whistleblowing concerns and investigations will be retained in for 6 years from the close of investigation. However, the Council's online record retention schedule does not specifically reference retention timeframes for whistleblowing disclosure / investigation papers.

Officers have confirmed that retention requirements were agreed with the Council's Information Governance Unit in June 2019, however, these have not yet been published within the online retention schedule.

2. Reporting inconsistencies

Review of whistleblowing investigation reports and associated committee reporting identified the following:

a) Report dates - examples of a small number of undated investigation and committee reports, and instances of inaccurate report dates were identified. Instances were also noted where date fields in standard reporting templates were blank. It is however acknowledged that the correct date can be traced by other references.

b) Internal Audit also encountered challenges following progress with one child protection whistleblowing disclosure raised in 2014, due to information on related individual disclosures (in this case an establishment) being consolidated and summarised at a high-level; involved officers no longer in post, and linked disclosures concerning senior officers being dealt with outwith the Whistleblowing team and central recording processes. Despite these challenges in identifying the information, we were able to confirm that the majority of management actions had been implemented.

c) Recommendations made in one investigation report were vague and did not clearly set out a course of SMART (Specific, Measurable, Achievable, Relevant and Time-bound) actions.

Risks

Regulatory and Legislative Compliance / Reputational Risk

- Lack of appropriate oversight on whistleblowing disclosures involving child protection.
- Limited assurance whistleblowing actions are completed in a timely manner.
- Records relating to whistleblowing disclosures may not be retained in line with retention requirements.
- Inaccurate / incomplete reporting to committee and citizens on whistleblowing disclosures.
- Recommendations made may not address root cause or prevent similar issues occurring.

Recommendations and Management Action Plan – Corporate Whistleblowing policy and procedures

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
1.1	Review of the Council's Whistleblowing policy and procedures should consider inclusion of the following as appropriate: a) Requirement for the Whistleblowing hotline provider to liaise with the Chief Social Work Officer and other parties as appropriate where it is unclear whether issues raised within whistleblowing disclosures fall under the scope of Child/Adult Protection procedures, and for such cases to be recorded within the central whistleblowing register and by Safecall as per the Tanner report. b) Formalising Executive Director roles and responsibilities for monitoring management actions arising from whistleblowing investigations; including notifying the Whistleblowing team of responsible officer allocation; target dates for implementing	The Whistleblowing Policy is being updated following the Tanner reviews and these changes will be implemented as part of this.	Richard Carr, Interim Executive Director of Corporate Services	Nick Smith, Service Director - Legal and Assurance Laura Callender, Governance Manager	31/03/2023

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
	actions; and when the Directorate action is complete. This should include a requirement to ensure adequate processes are in place to manage handover of outstanding actions when an action owner moves post or leaves employment with the Council. c) Quality assurance processes for investigation reports and associated committee reporting to ensure accuracy and consistency, including ensuring accurate dates are provided on all reports. d) Provision of guidance to investigating officers to support them making recommendations including ensuring recommendations are SMART (Specific, Measurable, Achievable, Relevant and Time-bound) and discussion with Directorates/Services to ensure recommendations are appropriate to the service. e) A standard reporting approach for whistleblowing action plans should be developed and communicated across all Directorates to ensure consistency and transparency in Committee reporting.			Nancy Brown, Programme Manager	
1.2	The Council's records retention schedule should be updated to include records retention requirements for whistleblowing disclosure and investigations records in line with those set out in the Whistleblowing policy.	Retention requirements will be included in the next version of the retention schedule due to be presented to the Corporate Leadership Team in October 2022 for approval.	Richard Carr, Interim Executive Director of Corporate Services	Nick Smith, Service Director - Legal and Assurance Kevin Wilbraham, Information Governance Manager Laura Callender, Governance Manager	31/12/2022

Finding 2 – Directorate Whistleblowing monitoring and reporting processes

Finding Rating	High Priority

1. Directorate monitoring processes

Review of processes established within directorates for monitoring progress with implementing whistleblowing recommendations highlighted the following:

a) Custom and practice has been for the Whistleblowing team to advise Directors of the recommendations and the proposed management actions following Committee, with the expectation and understanding that Directorates will implement them timeously.

b) Responsibility for ensuring actions are implemented and sustained is delegated to action owners within services, however, there is limited consolidated review and oversight of progress at Directorate level. Some Directorates advised that they considered this to be the role of the Whistleblowing Team.

c) Instructions outlined in emails sent by the Whistleblowing team are not consistently followed, with limited evidence that Directorates are proactive in confirming responsible officer details, or whether an action is complete, unless prompted by the Whistleblowing Team.

d) Implementation evidence is not routinely retained or held centrally. Obtaining sufficient evidence to demonstrate completion of actions for the audit sample took a number of weeks as it was provided by several different officers, and in some instances could not be provided as the action owner was no longer a Council employee.

Outcomes of previous internal audit reviews

A similar finding concerning the lack of clearly established processes for responsibility for completion of, and retention of evidence to support completion of, assurance actions was raised in the 'Implementation of Assurance Actions and Linkage to Annual Governance Statements' Internal Audit completed in July 2020. In August 2021, Directorates confirmed they would implement supporting processes which would include actions arising from monitoring officer reporting.

The findings in point 1 indicate that the design of processes established are inadequate and/or not operating effectively.

2. Directorate implementation of actions

Review of a sample of whistleblowing recommendations across all Directorates highlighted the following:

a) No progress on four recommendations for one whistleblowing disclosure from December 2020 to November 2021. The Whistleblowing team issued reminders; however, action owners were not identified by the service until prompted as part of this review in November 2021.

b) 13 actions for a further disclosure were reported as complete in December 2021, however further information or supporting evidence is required on 6 actions to adequately demonstrate these are fully complete in line with the investigating officer recommendations.

c) Action required for one recommendation was due to complete in Summer 2021, however, management advised this has since been delayed due to Covid-19. No further update has been provided to committee advising that completion of the action is delayed.

d) Three separate disclosures required action on disciplinary investigations, however, Learning and Development have no record of the action owners completing the Council's mandatory disciplinary learning modules.

3. Directorate reporting processes

Review of reporting processes highlighted the following inconsistencies in the use of action plans to monitor and report on whistleblowing related actions:

a) For one disclosure, an action plan was initially created by the Directorate and reported to Governance, Risk and Best Value Committee, as well as being tracked via the whistleblowing register in terms of closure of actions. It was noted however, that there has been no reporting to Committee by the Directorate on action plan progress since August 2020.

b) In contrast, for another disclosure an action plan was created by the Directorate and was monitored by an Executive Committee on a six-monthly basis. However, the actions were not tracked via the Council's whistleblowing register.

c) One instance was noted where the whistleblowing register, and summary table reported to the GRBV Committee omitted some wording from the original investigating officer's recommendation. Whilst the original recommendations were made available to the GRBV Committee when the investigation concluded, the officer revisions meant some context from the original recommendation was not tracked through to completion following Committee. The Whistleblowing team advise the wording was changed by the Service Director responsible for completion of the recommendations, and to prevent further occurrence, quality assurance processes were implemented to review accuracy of actions.

In addition, one instance was identified where an action owner, when prompted by Internal Audit for an update of progress, advised upon further consideration, that the investigating officer's recommendation was not appropriate for the service. This had not been communicated to the Whistleblowing Team or Committee.

Risks

The potential risks associated with our findings are:

Regulatory and Legislative Compliance / Reputational Risk

- Lack of clarity and understanding on roles and responsibilities at Directorate and service level.
- Limited assurance that management actions resulting from whistleblowing disclosures are fully implemented on a both a Directorate and Council wide level.
- Supporting evidence is not available to demonstrate completion of actions for related or further requirements.
- Inaccurate / incomplete reporting to committee and citizens on whistleblowing disclosures.

Recommendations and Management Action Plan – Directorate Whistleblowing monitoring and reporting processes

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
2.1	• Directorates should review the design and effectiveness of directorate level assurance monitoring processes established to ensure	Directorates will annotate the Whistleblowing Actions extract provided by the Governance Team with details of current action owners and target completion	Paul Lawrence, Executive Director of Place	All Place Service Directors	31/03/2023

	they include allocating, monitoring and reporting on whistleblowing actions. This should include recording all relevant disclosures and management actions within a central directorate register; and a requirement for action owners to provide regular updates on progress and supporting evidence to demonstrate actions are fully implemented. • Directorates should ensure they obtain sufficient assurance from action owners that actions are fully complete. It is recommended that Directorates retain supporting information and evidence for whistleblowing disclosures within a central file location or system (with adequate security settings to ensure confidentiality) to enable completeness and accuracy of records for reference/reporting, and for provision to Internal Audit in line with any further validation in line with GRBV requirements. • Handover arrangements should also be implemented and communicated to ensure a corporate history of the disclosure can be maintained when action owners leave employment with the Council. • Where disciplinary investigations are required as a result of whistleblowing disclosure recommendations, directorates should ensure Investigating Officers have completed the Council's mandatory disciplinary learning modules.	dates. This will be maintained on an ongoing basis and updated when individual action owners depart the organisation. Assurance will be sought from action owners as to completion of actions, with supporting information stored in a secure file location. This will be available on request to the IA team for the purposes of GRBV agreed implementation progress monitoring. Where disciplinary investigations are required as a result of whistleblowing disclosure recommendations, Investigating Officers will be required to complete the Council's mandatory disciplinary learning modules.	Richard Carr, Executive Director of Corporate Services Amanda Hatton, Executive Director of Education and Children's Services Judith Proctor, Chief Officer, Edinburgh Health and Social Care Partnership	Ross Murray, Operations Manager All Corporate Services Service Directors Layla Smith, Operations Manager Education and Children's Services Service Directors Gillian Tracey, Operations Manager All HSCP Service Directors Angela Brydon, Operations Manager	30/06/2023 31/03/2023 31/03/2023

2.2	• Directorates should adopt the standard reporting approach for whistleblowing action plans (refer recommendation 1.1e) to ensure consistency and transparency in Committee reporting. • Directorates should ensure the wording of investigating officer recommendations are not amended within reports/and or action plans, and where revisions are considered to be required these are reported to and approved by the Council's Whistleblowing team and GRBV Committee. • Directorates should establish arrangements to ensure that where a Service deems a previously agreed management action to be inappropriate or no longer relevant, this is reported to senior management, the Council's Whistleblowing team and GRBV Committee for transparency.	Directorates will implement the standard corporate reporting approach to whistleblowing action plans once this has been implemented and cascaded. Communications will be issued by Executive Directors to remind officers that the wording of recommendations should not be amended, and that where revisions are considered to be required or if an action is considered no longer appropriate, these are discussed with the Directorate Operations Manager and Whistleblowing Team and reported to GRBV as required.	Paul Lawrence, Executive Director of Place Richard Carr, Executive Director of Corporate Services Amanda Hatton, Executive Director of Education and Children's Services Judith Proctor, Chief Officer, Edinburgh Health and Social Care Partnership	All Place Service Directors Ross Murray, Operations Manager All Corporate Services Service Directors Layla Smith, Operations Manager Education and Children's Services Service Directors Gillian Tracey, Operations Manager All HSCP Service Directors Angela Brydon, Operations Manager	31/03/2024 31/12/2023 31/03/2024 31/03/2024

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Internal Audit Report

Payment Card Industry Data Security Standards Governance

22 July 2022

CS2108

Overall Assessment	**Significant improvement required**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Significant improvement required

Overall opinion and summary of findings

Significant and moderate control weaknesses were identified in the design and effectiveness of the control environment and governance and risk management arrangements established to ensure that the Council achieves compliance with PCI DSS requirements, with instances of non-compliance identified.

Consequently, only limited assurance can be provided that both the Council and associated partner organisations support the secure management of payment channels and cardholder data.

Our review established that the Council currently does not complete its own PCI DSS self-assessment questionnaire (SAQ) to assess compliance across all payment systems used by the Council, and shared drives where payment details could potentially be stored, instead relying solely on the Barclaycard and Worldpay payment provider SAQs to confirm ongoing PCI DSS compliance. As the Council accepts card payment transactions, it is subject to PCI DSS compliance although the handling, collection, processing, and storage of the protected cardholder data is outsourced, and should complete and submit its own annual SAQ in addition to those provided by the Barclaycard and Worldpay to confirm full ongoing compliance.

Additionally, no approved scanning vendor has been appointed by the Council to perform quarterly external vulnerability scans of the Council's networks in line with PCI DSS requirements. Whilst internal network vulnerability scans are performed by CGI (which is an additional PCI DSS requirement), their scope does not currently cover the full PCI Card Data Environment (CDE) requirements detailed in the standards.

Another area of concern relates to the volume of shadow IT applications used across the Council, as it is not currently possible to confirm whether any of these applications support card payment transactions, and (if so) the extent of their compliance with PCI DSS requirements. It is acknowledged that management is currently identifying the full population of shadow IT applications used and has implemented additional procurement controls to ensure that future purchases are identified and recorded.

We also noted that external website providers are sub-contracted by CGI to develop webpages that can include payment processes. Where this is the case, it is important to ensure that contractual arrangements agreed between CGI and the supplier include the requirement to ensure that website security controls are, and remain, aligned with PCI DSS requirements.

It is likely that these gaps have occurred as the Council's PCI DSS governance and risk management arrangements also need to be improved, with responsibilities for ensuring full end to end PCI compliance clearly defined and allocated, and ongoing compliance oversight provided by an appropriate governance forum.

The main risk associated with these findings is potential application of penalty fees and increased transaction fees by the acquiring bank (the Council's bank) where non-compliance and data breaches are identified. These penalties would be applied to the Council and can only be passed to third party payment providers where they are directly responsible for the compliance and / or data breaches. The Council would also require engaging a PCI Forensic Investigator (PFI) to establish the source of the breach which would incur additional costs.

There would also be potential reputational consequences in the event of breaches if citizens lose confidence in the Council's ability to protect their sensitive payment card information, with increased demands for alternative cash payment processes.

Management Response

The Council's Treasury Manager has historically been responsible for PCI DSS compliance.

Given the complexities associated with addressing findings and the need for collaboration across a number of services to agree ongoing ownership and responsibilities for the PCI DSS framework, a phased implementation approach will be adopted.

An implementation plan will be prepared by Treasury and Digital Services by 31 January 2023 for development of a PCI DSS Council wide framework that considers and addresses (where possible) the IA recommendations included in this report and will be agreed with all services and external stakeholders who will be required to support the process.

The plan will be shared with Internal Audit to confirm that appropriate actions have been defined, or risks accepted (where appropriate), and management actions will then be agreed based on the content of the plan, with their implementation progress monitored through the established Internal Audit follow-up process

Audit Assessment

Audit Areas	Findings	Priority Rating
• Governance and Oversight	1. Payment Card Industry Data Security Standards (PCI DSS) Governance Arrangements	High
• Supplier Management		
• Change Management	2. Third party contracts and supplier management	Medium
• Asset Management		
• Physical Security	3. Alignment between CGI contractual and PCI DSS requirements	Medium
• Cardholder Data (CHD) incident management	4. Point of Sale Device Security and Currency	Medium

Areas of good practice

The following areas of good practice have been identified:

- **Change Management Process** – there is a requirement for completion of data privacy impact assessments (DPIAs) for all planned significant process and technology changes to identify potential data privacy and security risks, with recommendations provided to ensure that they are addressed.
- **Shadow IT Applications –** the Council is in the process of identifying its full population of shadow IT applications and has implemented additional procurement controls to ensure that future purchases are identified and recorded.
- **Management of Asset Registers** - the council maintains asset registers for point of sale (PoS) devices procured through the Barclaycard and Worldpay that include their location; service owners; model details; and relevant payment provider, satisfying Requirement 9.9.1 of the PCI Standards.

Background and Scope

The Payment Card Industry Data Security Standards (PCI DSS) are the information security standards for organisations that accept card payments from major payment card providers such as Visa, MasterCard, Discover, JCB and American Express. Any organisation that accepts card payments must be compliant with PCI DSS standards to demonstrate that Cardholder Data (CHD) and other sensitive financial information is stored, processed and used securely.

PCI DSS consists of the following 12 requirements covering the security controls that interact with, or could otherwise impact the security of, CHD:

1. Protect your system with firewalls
2. Configure passwords and settings
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Regularly update and patch systems
7. Restrict access to cardholder data to business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to workplace and cardholder data
10. Implement logging and log management
11. Conduct vulnerability scans and penetration tests
12. Documentation and risk assessments

It is essential to maintain PCI DSS compliance to secure cardholder data where it is captured at the point of sale as it flows into the payment system, and to ensure that security threats and vulnerabilities are identified and addressed. This includes protecting card readers; point of sale terminals; networks and wireless access points; data storage and transmission infrastructure; paper-based records; and online payment applications.

PCI DSS Management across the Council

The Council's Treasury Manager is responsible for the Council's PCI DSS compliance, with the Council's main payment gateway (Barclaycard) and associated payment Chip and Pin devices with relevant services responsible for providing ongoing compliance guidance to their own teams.

The Treasury Manager is can also liaise with the Digital Services team and their technology partner CGI for ongoing technical support and guidance.

Some Council services use other payment gateways, including Culture and Wellbeing within the Place directorate for booking tickets; Parking payments (this system is provided by a third-party supplier); and the Gov.UK Pay system, which is used across the UK public sector to take payment for services and issue refunds.

Management has confirmed that an historic policy decision was taken that the Council would not hold any CHD to reduce the risks associated with potential non-PCI DSS compliance.

Instead, all relevant CHD is acquired and managed under contractual arrangements with Barclaycard, and the Treasury Manager manages the Barclaycard supplier relationship.

The Council's Externally Hosted "Cloud and Web" Services Protocol also confirms that there is no expectation for core Council systems to store credit card details requiring detailed PCI DSS compliance; that Council processes for accepting card payments must be compliant with PCI DSS; and that any externally hosted services that do hold CHD on the Council's behalf do need to be compliant with PCI DSS regulations.

Ongoing PCI DSS compliance is achieved by ensuring that appropriate redirection to the relevant Barclaycard hosted payment pages set up by the Council but owned by Barclaycard incorporated into online payment forms included in the Council's external website. When ready to accept payment details, a URL link is accessed, and card payment details taken securely by

Barclaycard, with a success or failure message generated on return to the payment form.

Mail and telephone order (MOTO) payments processed in the Customer Contact Centre are managed through the 'Red Box' telephony application where the telephone recording drops off to enable secure provision of payment card details to Barclaycard, and then re-engages.

Physical payments are collected through BarclayCard and WorldPay chip and pin point of sale devices that do not acquire or store CHD. A significant project was completed in December 2021 that migrated all online and telephony payments to the new Barclay card payment gateway (Smartpay Fuse).

Current Compliance

Management has confirmed that the Council completed a PCI DSS self-assessment in 2020/21 with Barclaycard and has also received confirmation of Barclaycard's own compliance with the standards (September 2021).

Future Plans

Replacement of all legacy Worldpay chip and pin devices (mainly used in educational and cultural venues) with Barclaycard terminals is planned.

Scope

The objective of this review was to assess the adequacy and effectiveness of the key controls established to ensure ongoing compliance with PCI DSS requirements designed to protect cardholder data that is acquired through the Council's website and Customer Contact Centres and processed, transmitted and stored by Barclaycard on behalf of the Council.

Risks

The review aims to provide assurance that the following Council enterprise risks are being effectively managed:

- Supplier, Contractor, and Partnership Management
- Technology and Information
- Governance and Decision Making
- Regulatory and Legislative Compliance
- Fraud and Serious Organised Crime

Limitations of Scope

The following areas were specifically excluded from the scope of this review:

- Review and testing of the configuration of network security controls such as firewalls, routers and other network infrastructure, as these areas were covered in the Network Management audit completed in August 2021.
- Security controls in place in shadow IT applications provided by third parties that are not managed by the Council's technology partner CGI.

Reporting Date

Our audit work concluded on 21 July 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Payment Card Industry Data Security Standards (PCI DSS) Governance Arrangements

Finding Rating	High Priority

The Council currently has no established governance arrangements to confirm ongoing compliance PCI DSS compliance requirements.

The Treasury team currently manages relationships with the Council's payment partners (Barclaycard and Worldpay) and directs any PCI and payment card queries to either Digital Services, or CGI, however, these responsibilities have not been formally clarified or confirmed.

Consequently:

1. Payment channels - the Council cannot confirm its full population of payment channels due to the volume of shadow IT systems historically procured by services that potentially include payment processes and are not supported by Digital Services and CGI.
2. Compliance assessments - PCI DSS compliance self-assessment questionnaires (SAQs) are received annually from the BarclayCard and WorldPay payment providers, however, there is currently no set schedule for completing these annual questionnaires.
3. Compliance assessments – the Council does not complete its own SAQs in addition to those completed by the payment providers to demonstrate ongoing annual PCI DSS compliance. This would involve providing details of established PCI DSS governance arrangements including details of relevant policies; procedures; roles; and responsibilities.
4. External Vulnerability Scans – an approved scanning vendor has not been appointed to complete quarterly external vulnerability scans, or scans of the Council's networks following significant changes in line with PCI DSS requirement 11.2.2, and 11.2.3.
5. PCI documentation - details of payment channels and payment processes are not consistently maintained. Payment channel information is established when designing and implementing new payment gateways (for example, the project documentation on Barclaycard), but is not maintained to reflect any subsequent changes to operational payment processes.
6. Incident management - response plans for managing PCI related security incidents across all systems (including Shadow IT applications) that accept and process payments have not been created.
7. Risk management - the risks associated with handling; managing; and transferring card holder data (CHD) and other sensitive payment information are not recorded in relevant service risk registers. It is expected that this would include the risks associated with mishandling / misusing CHD; collecting CHD over the phone; and transferring CHD through shadow IT systems.
8. Training and awareness - training on PCI requirements (including security requirements and handling of payment card data) has not been provided to all employees who handle customer payment card details in line with PCI requirements 9.9.3 and 12.6. Guidance on handling point of sale (PoS) devices is provided for some services, however, this is informal.

Risks

- **Governance and Decision Making** - unable to confirm ongoing compliance and PCI DSS risks, and incidents are effectively managed.
- **Regulatory and Legislative Compliance** - non-compliance with requirements in relation to quarterly external vulnerability scanning.
- **Financial and Budget Management** - risk of non-compliance fees applied by relevant payment card brands.
- **Reputational Risk** – adverse publicity associated with PCI DSS breaches

Recommendations and Management Action Plan – PCI DSS Governance Arrangements

Ref.	Recommendation
1.1	1. Appropriate PCI DSS governance arrangements should be established, with responsibility for ongoing compliance responsibilities allocated to an Executive, and Service Director. One potential governance solution could include extending the responsibility of the established Cyber and Information Security Steering Group to include PCI DSS compliance. 2. A RACI matrix that details those within the Council responsible; accountable; to be consulted; and informed should be prepared that describes PCI governance and compliance responsibilities, including completion of self-assessment questionnaires by both the Council (if required) and payment providers. 3. Current incident response plans should be reviewed to ensure appropriate responsibilities for assigning council and CGI colleagues to triage; manage; and remediate security incidents that impact payment information and assets are in place. 4. Relevant risks associated with PCI compliance should be identified; assessed; recorded in relevant service risk registers; and managed, with the most significant risks escalated to the new PCI DSS governance forum.
1.2	1. An assessment should be performed to determine the full population of payment channels used across the Council, including payments processed using any shadow IT applications, but excluding transactions processed by external payment providers. Note that a register of the shadow IT applications used across the Council is currently being established and will be maintained by Commercial and Procurement Services. This could be used as a reference point. 2. The payment processes and channels identified should be appropriately documented to include detailed payment collection methods (for example, point of sale / online / telephone order) for each channel, together with volumes of annual payment transactions. 3. Digital Services / Commercial and Procurement Services should provide details of all registered shadow IT procurement approvals for applications that include payment channels to colleagues responsible for ongoing PCI DSS compliance, to ensure that the full population of Council payment channels is completely and accurately maintained. 4. The Council should complete its own annual self-assessment questionnaire (SAQ) (in addition to those provided by external payment providers) in line with PCI DSS SAQ guidance to confirm ongoing PCI DSS compliance, and should engage with the payment providers and the acquiring bank (the Council's bank) to determine whether SAQ A (for use of websites that redirect to collect payment providers) and SAQ B (for use of point of sale terminals) should be completed. 5. An approved scanning vendor should be appointed to complete quarterly external vulnerability scans in line with PCI DSS requirements 11.2.2 and 11.2.3.
1.3	1. PCI DSS training should be commissioned and delivered to all employees who handle payment transactions in line with PCI requirements on secure handling of payment data and cards. 2. The training materials should include common threats associated with payment collection and processing, such as e-skimming and the risks associated with tampering with point of sale devices.

Finding 2 – Third party contracts and supplier management

Finding Rating	Medium Priority

1. CGI Third Party Supplier Management

Where services procure external website providers to develop webpages for Council services, and establish contracts to support ongoing hosting arrangements, CGI may become involved in ensuring that payment interfaces are built that redirect payments to the BarclayCard or WorldPay pages for payment collection, avoiding the need for the Council to collect; process; or store any cardholder payment data.

These external relationships are then either managed by services, or CGI on behalf of the Council and include:

- The experience outdoors; joinedinedinburgh; active schools; and mobile pay websites were independently sourced by services who manage ongoing website hosting directly with these external providers. CGI involvement was developing the Barclaycard payment interface for these websites.
- Planning and Building Standards – this is a Scotland wide portal which was developed by the Scottish Government (SG), with only the Barclaycard payment interface being jointly developed by the SG and CGI for the Council.
- Verint / Redbox – the Verint customer relationship management (CRM) system and Redbox solution (used to prevent recording of payment details) is managed by both CGI and their subcontractor Commsworld.
- Gov.pay – this payment system is an addition to the Verint CRM system. The system is provided and managed by the UK Government.
- Parking – NSL provides the web-based systems used to support payment of parking fees and charges.

Our review of a sample of these contracts confirmed that:

- whilst these contracts include information security requirements, they are not fully aligned with PCI DSS security requirements.
- there are no contractual requirements for external suppliers and / or CGI to maintain security controls that are aligned with PCI DSS requirements for the systems referred to above.

It is acknowledged that CGI has established compensating controls (for example ongoing vulnerability scanning and security monitoring through the established Security Operations Centre) that should be able to identify any potential security threats or issues that arise from these third party hosted web pages. Third party sites in this instance, are the council sites that are built by third party web developers where CGI were involved for onboarding and management.

- **Shadow IT Payment Services**

Whilst the full population of shadow IT applications currently used by the Council to accept payments is currently unknown, existing guidance on procurement contracts and ongoing management of shadow IT applications does not highlight the need to ensure both initial and ongoing compliance with PCI DSS requirements where payments are accepted via shadow IT systems.

Risks

- **Supplier, Contractor and Partnership Management** - guidance on supplier contracts and ongoing supplier management does not include the requirement to consider ongoing PCI DSS compliance.
- **Technology and Information** –weaknesses in supplier's infrastructure that could potentially compromise the redirect to payment providers, or that the website providers do not inadvertently store; process; or misuse payment card data.
- **Regulatory and Legislative Compliance** - the council does not meet PCI DSS requirements.
- **Financial and Budget Management** - potential risk of non-compliance fees applied by relevant payment card brands.
- **Reputational Risk** – adverse publicity associated with PCI DSS breaches.

Recommendations and Management Action Plan – Third party contracts and supplier management

Ref.	Recommendation
2.1	The established CGI and relevant third-party provider contracts should be reviewed and updated to include: 1. responsibility for ensuring that third party security arrangements for websites that include redirection links to payment providers are appropriately secured in line with established PCI DSS security requirements. 2. the requirement to obtain ongoing assurance from third parties that their security arrangements remain aligned with PCI DSS requirements and provide confirmation of ongoing third-party compliance to the Council.
2.2	Existing guidance on procurement contracts and ongoing management of shadow IT applications should be updated to reinforce the need to: 1. ensure that procurement contracts for all shadow IT applications currently used by the Council to accept payments include the requirement to implement and maintain security arrangements that are aligned with PCI DSS standards. 2. obtain ongoing assurance from third parties that their security arrangements remain aligned with PCI DSS requirements and provide confirmation of ongoing third-party compliance to colleagues responsible for ongoing PCI DSS governance.

Finding 3 – Alignment between CGI contractual and PCI DSS requirements

Finding Rating	Medium Priority

Whilst services provided by CGI to the Council are aligned with some aspects of PCI DSS requirements (for example, managing firewall configuration; network access controls; external connections; whitelisting connections; and formal security change management processes) they are not fully aligned with the following requirements:

- Discovery exercises to identify card holder details inadvertently stored in Council network folders or applications or data stores;
- Quarterly internal vulnerability scans (or scans following implementation of significant changes) and annual penetration tests that cover the full PCI Card Data Environment (CDE) requirements, such as connections between point of sale devices and payment gateways accessed via the Council's networks as required by PCI DSS requirement 11.2.1; 11.2.3; and 11.3.1.
- Quarterly wireless analyser scans to detect and identify all authorised and unauthorised wireless access points as required by PCI DSS requirement 11.1 (1 – 2).

Risks

- **Technology and Information** - unauthorised wireless access points and vulnerabilities in connections between point of sale devices and payment gateways are not identified and remediated.
- **Regulatory and Legislative Compliance** - the council does not meet PCI DSS security requirements.
- **Financial and Budget Management** - potential risk of non-compliance fees applied by relevant payment card brands.
- **Reputational Risk** – adverse publicity associated with PCI DSS breaches.

Recommendations and Management Action Plan – Alignment between CGI contractual and PCI DSS requirements

Ref.	Recommendation
3.1	The established CGI contract should be reviewed and updated to: 1. ensure that CGI contractual and PCI DSS security requirements are consistently aligned with completion of quarterly internal vulnerability scans (or scans following significant change) and annual penetration tests that cover the full PCI card data environment in line with PCI DSS requirements 11.2.1; 11.2.3; and 11.3.1. 2. establish a PCI DSS security breach reporting process where breaches are reported to the relevant PCI DSS governance forum. 3. request CGI to provide annual assurance on compliance with PCI DSS requirements to support submission of Council annual self-assessment questionnaires.

Finding 4 – Point of Sale Device Security and Currency

Finding Rating	Medium Priority

1. **Secure Point of Sale Connectivity** - the security of point of sale (PoS) connections that connect to Barclaycard and Worldpay through independent Wi-Fi routers that are not managed by CGI cannot be confirmed as they have not been independently tested.

   Management has advised that it is Barclaycard and Worldpay's contractual obligation to ensure that these devices connect securely to their hosts.
2. **Unapproved PoS models** -Some PoS models used by the Council (IWL250, iCT200, vx680 and vx820) are not listed in the PCI approved PTS device list.

   Whilst PCI DSS does not specify that only PCI PTS-approved devices can be used, some payment brands (for example VISA or Mastercard) have their own requirements for using PTS-approved devices, including whether PTS devices with expired approvals can be used.
3. **Physical security controls** - physical security controls that should be applied consistently to safeguard PoS devices (for example, securing in locked cabinets) have not been defined and documented, in contravention of Requirements 9.9.3 and 12.6.

Risks

- **Technology and Information** - risk of point-of-sale (PoS) device firmware being open to exploitation by hackers as no tests or scans have been performed to confirm that they are running on up-to-date patches and security controls.
- **Technology and Information** - non-approved devices may not be fit for purpose or may have an inherent fault meaning they are at a higher security risk level as they may not be able to withstand the latest generations of attacks. This risk is exacerbated as non-approved devices do not receive ongoing maintenance and service updates from the payment provider.
- **Fraud and Serious Organised Crime** - unsecured PoS assets could be stolen or used inappropriately
- **Regulatory and Legislative Compliance** - the council does not currently meet the PCI DSS requirements
- **Financial and Budget Management** - potential risk of non-compliance fees applied by relevant payment card brands.
- **Reputational Risk –** adverse publicity associated with PCI DSS breaches

Recommendations and Management Action Plan – Point of Sale Device Security and Currency

Ref.	Recommendation
4.1	The implementation plan developed by Treasury and Digital Services should set out responsibilities for ongoing PCI DSS governance activities including: 1. request payment providers (Barclaycard and Worldpay) to provide ongoing assurance that point-of-sale devices (PoS) are running on the latest software.

	Payment providers should be pushing software updates out to devices as part of their ongoing compliance activities, but it is recommended that the Council obtains ongoing assurance in this area. 2. engage with merchant acquirers or payment brands to advise them of the expired PoS devices currently in use and discuss potential implications. 3. develop plans to replace all non-approved PoS devices currently used by the Council. 4. confirm whether new payment devices are approved versions in line with the PCI PTS listing and determine when approvals expire.

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Internal Audit Report
Planning and Performance Framework – Design Review

30 June 2022

CS2109

Overall Assessment	**Some Improvement Required**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Some Improvement Required

Overall opinion and summary of findings

Whilst some moderate control weaknesses were identified in the design of the key controls supporting the newly developed integrated planning and performance framework, they provide reasonable assurance that risks associated with the design of the framework are being managed, and that the Council's objectives to implement an appropriately designed framework to support ongoing monitoring of business plan delivery should be achieved.

The design of the planning and performance framework is dependent on first line Council directorates and divisions providing complete and accurate source data to support calculation of KPIs and performance benchmarks and preparation of performance reports by the Data, Performance and Business Planning team ('DP&BP team'), with significant reliance on first line Information Asset Owners (IAOs) to ensure that this is consistently achieved

Our High rated finding highlights this risk and includes some recommendations that, if implemented, should provide ongoing assurance on the completeness and accuracy of high-risk data that, if incomplete or inaccurate, could have a significant impact on the content and accuracy of performance reports.

Our Medium finding highlights the need to make improvements to the design of operational performance reporting processes that will be applied by the DP&BP team. These include ensuring that data and formulae included in key performance reporting spreadsheet models is appropriately protected.

Finally, our Low rated finding recommends that data quality performance objectives are defined and consistently applied in first line directorates and divisions involved in extracting and providing source performance data to the DP&BP team for inclusion in performance reports.

Audit Assessment

Audit Areas	Findings	Priority Rating	Areas of good practice
• Development of performance metrics and methodology	1. Completeness and Accuracy of Divisional Source Performance Data	High	Our review identified that good progress is evident with the identification of relevant performance KPIs and benchmarks, and that the framework has been designed to support and encourage a culture of continuous improvement and data-based decision making within the Council. The following specific areas of good practice were also noted: • Significant research is evident in the design of the framework (which includes the "plan; do; check; and act" methodology) and identified best practice approaches have been incorporated in the creation of performance reporting KPIs; metrics; and milestones. • Good engagement has been carried out with senior Council staff and elected members in order to produce the framework. This included an initial briefing to Policy and Sustainability on the proposed approach, followed by a final paper setting out the
• Strategic Change and Delivery (second line) Data quality	2. Design of Performance Framework Operational Processes	Medium	

• Performance monitoring and reporting • Data protection	3. Directorates and Divisional Data Quality Objectives	**Low**	full planning and performance framework. As part of the design, meetings were held with all political groups and a workshop was arranged with the Governance, Risk and Best Value Committee. Meetings were also held with the Wider Leadership Team and the Corporate Leadership Team was closely involved in the design of framework. Positive feedback on the framework design has been received from both officers and elected members. • The benchmarks chosen for the KPIs are aligned with the Local Government Benchmarking Framework. • The framework addresses a number of observations detailed in Audit Scotland's Best Value Assurance Report of the City of Edinburgh Council in 2020. • Management intends to create a 'Data Dictionary' or 'single source of truth' that will include detailed performance metric calculations; their owners; and relevant data sources that will be shared across all relevant Council stakeholders.

Background and Scope

The Council's new business plan titled 'Our Future Council, Our Future City', covering three-year period 2021-2024, brings together the Council's three priorities of tackling poverty and inequality; boosting sustainability; and enhancing wellbeing. The plan includes fifteen outcomes and actions that will help to successfully deliver these priorities for the citizens of Edinburgh and its visitors.

It is essential that high level strategic performance objectives and priorities are established and communicated across the Council to support the business plan delivery. These should then be supported by divisional delivery performance objectives together with clearly defined employee expectations, and ongoing performance monitoring and reporting to confirm whether objectives are being consistently achieved. Planning and performance frameworks achieve this by creating a 'golden thread' that consolidates collective performance across organisation to determine progress towards delivery of strategic objectives.

The Council's new Performance Framework

An integrated planning and performance framework has been developed by the Data, Performance and Business Planning team ('DP&BP team') to support delivery of the business plan. The framework design is based on the 'plan, do, check, review, and act' performance cycle, with the objective of enabling effective performance discussions across all divisions and driving a continuous improvement culture.

The framework design involves analysing and presenting a combination of external data (for example from the Scottish Government), and internal data from a combination of the DP&BP team and Council divisions.

Data will be received by a generic team email, system generated reports, or manual data extraction from systems, that will be analysed and consolidated to produce data trend performance reports using the appropriate Business Intelligence application. A 'Data Dictionary' that details all KPI calculations is included in the design and is in the next phase of development, not covered by this audit.

The performance reports will assess ongoing strategic delivery progress in comparison to a range of specific performance milestones and SMART (Specific, Measurable, Achievable, Relevant, and Timebound) key performance indicators (KPIs) that are aligned to each of the 15 Business Plan outcomes.

Performance reports will be produced regularly to support both management decision making at all levels across the Council and elected member scrutiny, and the Council's main KPIs will also be published on the Council's website.

The new performance monitoring framework will see a shift from performance reporting based on single data points, which provide only a snapshot in time, towards data trend analysis.

A phased rollout of the performance framework has commenced across Directorates and the first performance report will be brought to the Policy and Sustainability Committee in November 2021.

Information Management Across the Council

Discussion with the Information Governance team has confirmed that the Council currently applies a devolved approach to managing information, with first line directorates and divisions responsible for managing their information assets. Information Asset Owners (division directors) are ultimately responsible for identifying and addressing any risks relating to their information and ensuring ongoing compliance with the Council's information governance policies. IAOs are supported in delivering these responsibilities by System Administrators who should have authority to apply relevant information governance rules, including updating Council data and records to ensure their integrity and quality. Further detail is included on the Orb.

Scope

This review assessed the design of the key controls supporting the newly developed integrated planning and performance framework.

Testing was performed across the period May 2021 to June 2021.

Risks

The review also provides assurance in relation to the following Corporate Leadership Team (CLT) risks:

- Strategic Delivery
- Financial and Budget Management
- Technology and Information
- Governance and Decision Making
- Service Delivery

Limitations of Scope

The scope of this review was limited to assessing the design of the new planning and performance framework prior to its implementation.

Both the effectiveness of the implementation process and the use of the framework by Council divisions and directorates were specifically excluded from our scope.

Existing data quality checks performed by first line teams on the performance data submitted to support consolidated performance reporting were also specifically excluded from our scope, however, the design of data quality checks performed by the second line Change and Delivery Team were included.

It is likely that a further review of the effectiveness of the performance framework will be completed once it has been embedded operationally across the Council that will include the data quality checks performed by first line teams.

Internal Audit recommendations included in this report will not be applied to the Health and Social Care Partnership as they have established their own performance framework.

Reporting Date

Our audit work concluded on 29 June 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Completeness and Accuracy of Divisional Source Performance Data

Finding Rating	High

The Data, Performance and Business Planning team (DP&BP team) confirmed that whilst a sense check is performed on source performance data received from divisions, there are no detailed quality assurance checks to confirm its completeness and accuracy.

Instead, reliance will be placed on the Council's first line Information Asset Owners (IAOs) and System Administrators to manage their information assets appropriately and confirm the completeness and accuracy of the performance data provided, with the DP&BP team highlighting significant variances in expected metrics and historic trends, where further first line investigation is required.

Additionally, no assessment has yet been performed to identify high risk first line data that, if incomplete or inaccurate, could potentially result in both inaccurate KPI outcomes and incorrect progress reporting on business plan delivery.

Management has advised that data quality is a recognised issue across the Council, and that the Information Board has been established with the objective of reviewing and addressing these known data quality concerns

Risks

- **Technology and Information** – incomplete and/or inaccurate data is used as the basis for performance reporting;
- **Governance and Decision making** – incomplete and/or inaccurate data provided and used for decision making and scrutiny;
- **Strategic Delivery** – delivery of the business plan is impacted due to inappropriate strategic decisions based on incomplete/inaccurate data;
- **Service Delivery** – is impacted due to inappropriate operational decisions based on incomplete/ inaccurate data, and the inability to identify and resolve underlying performance issues; and
- **Reputational Risk** – reputational damage associated with inability to deliver the business plan and Council services to the expected standards

Recommendations and Management Action Plan – Completeness and Accuracy of Divisional Source Performance Data

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
1.1	a. The DP&BP team should provide standardised guidance to first line directorates and divisions on how data for the Planning and Performance Framework	a. This recommendation will be implemented as recommended by Internal Audit.	Richard Carr, Interim Executive Director of	Gillie Severin, Head of Strategic Change and Delivery	a. 30/09/2022 b. 28/02/2023

	should be extracted; analysed; collated; and submitted to the DP&BP team. This should include, but not be limited to guidance on how to: • Review and cleanse data; • Reconciliation controls that should be applied to support data extraction and confirm its completeness; • Data analysis controls (especially when using spreadsheet models); • The importance of appropriate quality assurance checks and review prior to submission; and • The process for submitting data (use of the generic DP&BP team email address). b. Directorates and divisions should be requested to confirm, at an appropriate frequency, that the guidance provided is being consistently applied, and proactively advise if there have been any changes to and/or significant issues with the process.	b. A questionnaire will be designed based on the guidance provided and will be issued to divisions annually, in line with the requirement to provide annual assurance framework submissions, to provide assurance that they are performing data extraction; analysis; collation; and submission in line with original guidance from the DP&BP team. Responses will be reviewed and considered as part of recommendation 1.3 below	Corporate Services	Edel McManus, Change & Delivery Manager Catherine Stewart, Lead Change and Delivery Officer	

1.2	Directorates and divisions should: 1. Incorporate the guidance provided by the Data, Performance and Business Planning (DP&BP) team into established processes to support the completeness and accuracy of high-risk divisional data to be provided for inclusion in performance reporting; 2. Ensure that these checks are consistently and effectively applied; 3. Take appropriate actions to address any data quality issues identified and ensure that these are included (where appropriate) in divisional risk registers. 4. Provide confirmation to the DP&BP team that the guidance is being consistently applied within agreed timeframes.	a. The guidance will be applied when issued by DP&BP team and dip sampling of data returns will be undertaken on a quarterly basis via the Directorate Assurance Officer to provide assurance that guidance is being applied. This will be aligned to required reporting to the Directorate Quarterly Performance and Assurance Meetings between the Divisions and the Executive Director. b. The guidance will be reviewed, and relevant elements applied when issued by DP&BP team and dip sampling of data returns will be undertaken on a regular basis via the Directorate Assurance Officer to provide assurance that guidance is being applied. c. ECS will implement dashboards at each level of the organisation and will also undertake case file audits, in which a percentage per month will be randomly selected across Audits, Thematic multi-agency audits, Complaints and complements, Reviews, Data, Voice – individual and group, Research and practice wisdom, Line of sight activity, in order to test for data quality. This will be a mirror of regulation 44 when reports are compiled to ensure that the children are being kept safe and how well their wellbeing is being promoted.	a. Richard Carr, Interim Executive Director of Corporate Services b. Paul Lawrence, Executive Director of Place c. Amanda Hatton, Executive Director of Education and Children's Services	a. Hugh Dunn, Service Director: Finance and Procurement Nicola Harvey, Service Director: Customer and Digital Services Katy Miller, Service Director: Human Resources Nick Smith, Service Director: Legal and Assurance	a. 30/09/2023 b. 30/09/2022 c. 30/09/2023

1.3	The DP&BP team should: 1. Complete a risk assessment on the source performance data provided by first line divisions to identify the high-risk data that (if incomplete or inaccurate) could have a significant impact on performance reports. It is recommended that source data should be assessed as either high; medium; or low risk with supporting rationale provided for these classifications; 2. Establish whether any first line checks are currently performed to confirm the completeness and accuracy of this data and (if so) whether these checks are adequately designed and consistently performed; 3. Where no first line checks are currently performed, agree with first line divisions the nature and frequency of checks that will be performed to confirm the completeness and accuracy of first line data; 4. Obtain confirmation from directorates and divisions that agreed data checks have been completed and that the data provided is complete and accurate, or obtain details of any inaccuracies identified and corrective actions; and 5. Include appropriate caveats in performance reports where any data inaccuracies have been identified.	A phased approach will be applied to implementation of these recommendations, recognising that circa one year will be required to assess the quality of data provided by divisions for performance reports. Once the process has been applied for a full year, a review will be performed by the DP&BP team to identify potentially high-risk data or divisions where additional support is required based on the outcomes of the survey (refer to Recommendation 1.1 above), and an action plan will be developed and discussed with IA.	Richard Carr, Interim Executive Director of Corporate Services	Gillie Severin, Head of Strategic Change and Delivery Edel McManus, Change & Delivery Manager Catherine Stewart, Lead Change and Delivery Officer	31/03/2023

Finding 2 – Design of Performance Framework Operational Processes

Finding Rating	Medium Priority

Review of the performance framework operational process design that will be applied by the Data, Performance and Business Planning (DP&BP) team in comparison with good practice, established that:

1. a detailed performance reporting timetable has not yet been created to ensure that divisions produce and provide data on time for inclusion in performance reports. Management has advised that a timeline is part of the implementation phase.
2. some source data for inclusion in performance reports will be provided by divisions via email to a group email address.
3. written processes for DP&BP data validation and cleansing have not yet been established but are part of the implementation phase.
4. collation and analysis of data used to calculate key performance indicators (KPIs) and prepare performance reports involves a significant amount of manual intervention from the DP&BP team
5. KPI spreadsheet formulae and contents are not protected by cell protection to prevent inadvertent or erroneous changes.
6. a change log has not yet been developed to record any changes made to KPI spreadsheet formulae and contents. Management has advised that this will be delivered as part of the design of the planned data dictionary.

Risks

- **Technology and Information** – incomplete and/or inaccurate KPIs and performance data is used to produce performance reports
- **Service Delivery** – performance reports are not delivered on time and to the expected level of quality.

Recommendations and Management Action Plan – Design of Performance Framework Operational Processes

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
2.1	The DP&BP team should: 1. establish and agree a detailed timetable with directorates and divisions that includes timeframes for provision of source data for inclusion in performance reports; 2. establish a process (where feasible), where secure network folders or another suitable alternative (for example a SharePoint site) accessible by the DP&BP	As part of the implementation of the Planning and Performance Framework, the DP&BP team will establish a detailed performance reporting timetable for first line directorates and divisions that will include timeframes for the provision of source data to the DP&BP team for inclusion in performance reports. All data received by email from divisions will be sent to a group email inbox as detailed in	Richard Carr, Interim Executive Director of Corporate Services	Gillie Severin, Head of Strategic Change and Delivery Edel McManus, Change & Delivery Manager Catherine Stewart, Lead Change	31/12/2022

	team and relevant first line divisional team members are used to support both provision and storage of first line performance data, avoiding use of email submissions (where possible).	recommendation 1.1. Any emails sent directly to officers will be sent a reply request submission of future data via the group inbox.		and Delivery Officer	
2.2	The DP&BP team should: 1. document data validation and cleansing processes that they will apply to deliver performance reports, and ensure that they are consistently applied; 2. ensure that all manual data collation and analysis processes are documented and consistently applied; 3. document all key performance indicator (KPI) and other performance metric calculations and ensure that they are consistently applied; 4. establish appropriate change control processes to support ongoing maintenance of operational procedures and any changes to KPIs and other performance metrics; 5. design and implement cell protection (where required) to ensure that source data and key formulae required to calculate KPIs, and other performance metrics cannot be inadvertently overwritten or changed.	The DP&BP team will document the cleansing guidance and the manual data collation and analysis processes and ensure these are consistently applied by the team. The proposed data dictionary will document all KPIs and other performance metric calculations and will be the only calculations applied. The data dictionary will also act as a change log to capture any changes to the KPIs and other performance metrics and will include details of the original calculation and source data, the date of change, and how the change was authorised. Finally, the Team will also ensure that the KPI spreadsheet formulae and data are protected to prevent inadvertent changes being made	Richard Carr, Interim Executive Director of Corporate Services	Gillie Severin, Head of Strategic Change and Delivery Edel McManus, Change & Delivery Manager Catherine Stewart, Lead Change and Delivery Officer	31/03/2023

Finding Rating	Low Priority

Finding 3 – Directorates and Divisional Data Quality Objectives

Data quality performance objectives for directorates and divisions involved in managing, extracting, and providing performance data to the Data, Performance and Business Planning team (DP&BP team) for inclusion in performance reports, have not yet been defined.

Risks

Service Delivery – receipt of poor-quality source data from first line divisions leading to potentially inaccurate/incomplete performance reports.

Recommendations and Management Action Plan – Directorates and Divisional Data Quality Objectives

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
3.1	The DP&BP team should: 1. design a SMART (specific; measurable; achievable; realistic; and timebound) data quality objective for Directorates and Divisions involved in managing and providing source data for inclusion in performance reports. 2. the objective should include being clear that services are responsible and accountable for data quality in their teams. 3. communicate the data quality objective to Service Directors for their information and use	The DP&BP team will prepare data quality objectives and share with directorates and divisions involved in provision of data for inclusion in performance report for discussion and agreement.	Richard Carr, Interim Executive Director of Corporate Services	Gillie Severin, Head of Strategic Change and Delivery Edel McManus, Change & Delivery Manager Catherine Stewart, Lead Change and Delivery Officer	31/12/2022
3.2	First line directorates and divisions should ensure that: 1. the performance reporting objective designed by the DP&BP team are considered and (where appropriate) incorporated into annual service plans and Performance processes; and	a. The Corporate Services Directorate will continue to work closely with the DP&BP Team on the relevant performance reporting objectives, keeping these under regular consideration and review, and where	a. Richard Carr, Interim Executive Director of Corporate Services b. Paul	a. Hugh Dunn, Service Director: Finance and Procurement Nicola Harvey, Service Director:	a.30/09/2023 b.30/09/2023 c.30/09/2023

	2. any capacity and/or performance challenges associated with data management are discussed with the DP&BP team.	appropriate will incorporate these into our Annual Service Plans. Regular discussions will take place with the DP&BP Team to consider any capacity and/or performance challenges associated with data management. b. Performance reporting objectives designed by the DP&BP team will be considered and (where appropriate) incorporated into the Place Annual Service Plan. Achievement of these objectives will be closely monitored with performance challenges associated with data management discussed with the DP&BP team. c. ECS will integrate Performance reporting objectives designed by the DP&BP i.e. PoaP in collaboration with the Change & Culture Framework to achieve clarity of targets so everyone can see their role in delivering data quality, including rigorous monitoring of progress towards impacts, ability to highlight and celebrate success, risk mitigation and management.	Lawrence, Executive Director of Place c. Amanda Hatton, Executive Director of Education and Children's Services	Customer and Digital Services Katy Miller, Service Director: Human Resources Nick Smith, Service Director: Legal and Assurance b. Ross Murray, Operations Manager – Place; Alison Coburn, Operations Manager, Place c. Gillian Tracey, Education and Children's Services Operations Manager	

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Internal Audit Report

Vulnerability Management
(Corporate, Learning & Teaching and Peoples Networks)

CS2102

28 September 2022

Overall Assessment	**Significant improvement required**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Significant Improvement Required

Overall opinion and summary of findings

Significant and moderate weaknesses were identified in both the design and effectiveness of the control environment supporting ongoing vulnerability management and remediation across the three networks operated by the Council and managed in partnership with CGI. Consequently, only limited assurance can be provided that security risks are being effectively managed and that the Council's objectives of maintaining secure network operating environments can be achieved.

Scanning an organisation's entire technology estate is essential and is the foundation of a good vulnerability management program, as vulnerabilities can exist in any system and cannot be addressed unless they are identified. Additionally, once an attacker breaches the security supporting one system, it can be used as a foothold to move laterally across the network and launch further attacks.

Our review confirmed that there are gaps in the coverage of monthly vulnerability scans as there are no established controls to confirm that the full network range is scanned; and no integration between the Configuration Management Database (CMDB) (the Council's central asset repository) and the vulnerability scanning systems used, with no manual reconciliation performed to confirm completeness of assets to be scanned prior to their initiation.

Additionally, review of the content of the CMDB confirmed that information about Council assets (mainly critical IP address information for static IP devices) is not included, which impacts the completeness and effectiveness of scanning.

CGI does perform a monthly network discovery scan to identify active network assets and subsequently scans them to identify potential vulnerabilities. Whilst this is a good practice vulnerability management approach, lack of assurance on completeness of the network range limits the effectiveness of this process, as assets could be active on other areas of the network that may not have been included in the scan.

We also identified the need to improve the vulnerability remediation process as system patching is not currently prioritised based on system criticality, as this requirement is not specified in the established CGI contract and noted that timeframes for application of recently released patches to critical systems by CGI are presently unclear.

Our final finding highlights the need for CGI to establish and implement an exception tracking process that records and monitors the unique and cumulative risks associated with approving short-term exceptions from established Council security policies and standards and ensures that all approved exceptions are subsequently closed.

It is important to ensure that these findings are addressed as independent assessors who assess the vulnerability of networks to support both Cyber Essentials Plus and Public Services Network compliance complete their independent testing based on details of the technology estate maintained by CGI on behalf of the Council.

Audit Assessment

Audit Areas	Findings	Priority Rating		Areas of good practice
• Performance and Oversight	1. Incomplete vulnerability scanning coverage	**High**		The following areas of good practice were identified: 1. Patch Management – there is a defined patch cycle for technology assets, and appropriate change management practices are applied to support patching and other updates to asset operating systems. 2. Gold Images and Baselines - End User Devices (laptops/desktops), Windows & Unix server systems have standard gold images with Centre for Internet Security (CIS) controls applied as part of baseline practice. These images are reviewed and approved by the CGI Information security team before being rolled out across the estate. However, it was identified from previous audits that baseline images for network devices such as firewalls, routers were not maintained as identified in the Network Security review performed in 2021. 3. Governance and oversight – Regular engagement is evident between CGI and the Council to review the vulnerability management reports and patching performance. Monthly technology currency meetings are established to review, plan and mitigate against risks introduced by end of life and end of support systems.
• Asset Management	2. Vulnerability prioritisation and remediation	**Medium**		
• Vulnerability Management				
• Change Management	3.Security policy exception management	**Medium**		

Background and Scope

Modern technology systems contain vulnerabilities either due to software defects that require patches to remedy or due to configuration issues. These vulnerabilities could be used by an attacker to gain unauthorised access to systems and data leading to disruption to Council services and/or a breach of staff, client or other data. As vulnerabilities are being discovered all the time, the Council needs a robust vulnerability management process to manage the risk that vulnerabilities present.

Vulnerability Management across the Council

The City of Edinburgh Council (the Council) currently utilises three separate networks, namely the corporate network (which is used by a majority of Council divisions), the learning and teaching (L&T) network (which is used by the schools) and the Peoples network (used by libraries)

The networks are segregated and separately managed and maintained by the Council's technology partner CGI, with the Council's Digital Services team providing oversight by obtaining assurance over network performance and security.

Regular vulnerability scanning has been implemented for all three networks and is performed by CGI. The design of the vulnerability scanning includes all assets with an IP address that are recorded in the Configuration Management Database (CMDB) maintained by CGI.

In addition, the corporate network is scanned by an independent third party as part of maintaining ongoing compliance with the UK Government's Public Services Network (PSN) accreditation and Cyber Essentials Plus (CE+) accreditation.

All vulnerabilities identified from these scans are then considered and reviewed by Digital Services and CGI and outcomes shared with the UK Government Cabinet Office to support the PSN accreditation process. Confirmation is also provided to the Scottish Government that the independent CREST accredited organisation who performed the scan has awarded the CE plus accreditation.

The Council's Digital Services cyber security team and CGI colleagues oversee the vulnerability scanning and remediation services provided by CGI through ongoing review of security metrics and vulnerability management reports provided by CGI.

The process supporting ongoing management and remediation of vulnerabilities across Corporate, L&T and Peoples network are similar, with minor variations in relation to end user devices normally connected to the Peoples network, primarily due to the Council's Covid-19 response.

Scope

This review assessed the adequacy of the design and operating effectiveness of the key vulnerability management controls to ensure effective management and remediation of vulnerabilities identified across the three networks managed by the Council.

This review has been performed by exercising the 'right to audit' clause included in the CGI contract.

Limitations of Scope

No additional vulnerability scanning, or penetration testing has been performed across the Council's networks.

We recognise that libraries were, and some still remain closed as part of the Council's Covid-19 resilience response, the review has focused on plans to reinstate vulnerability scanning across the Peoples network and libraries that have now reopened.

Reporting Date

Our audit work concluded on 26 August 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Incomplete vulnerability scanning coverage

Finding Rating	High Priority

Corporate and Learning and Teaching vulnerability scans - review of a sample of 23 assets used across the Corporate and Learning and Teaching networks sourced from the Configuration Management DataBase (CMDB) (the central repository for all Council technology assets with an IP address to be included in ongoing vulnerability scans) confirmed that 14 of the assets were excluded from the March 2022 vulnerability scan.

The missing assets included end user devices; servers; and firewalls. Further investigation confirmed that these devices were excluded due to:

Network range completeness: vulnerability scan network ranges are updated quarterly, however, there are no established controls to ensure that there is 100% coverage of the current network environment and confirm that there are no exclusions or exceptions to the scan.

Incomplete CMDB content: the CMDB does not include critical IP address information for static IP devices, resulting in gaps in the completeness of the scanning operation.

CMDB alignment: there is currently no reconciliation performed between CMDB content, and the assets included in monthly vulnerability scans.

CGI management has confirmed that this reconciliation is performed for other CGI clients to confirm that vulnerability scans are complete.

It is acknowledged that CGI performs a monthly network discovery scan to identify active network assets, and subsequently scans them to identify potential vulnerabilities. Whilst this is a good practice vulnerability management approach, lack of assurance on completeness of the network range limits the effectiveness of this process.

Additionally, if the full population of Council assets is not recorded in the CMDB, this will present challenges when investigating security incidents.

Risks

Technology and Information

- Potential risk of cyber-attack due to incomplete vulnerability scanning coverage across the network environment and network assets as potential vulnerabilities cannot be identified and remediated.
- Inability to complete security incident investigations if CMDB content is incomplete.

Recommendations and Management Action Plan – Incomplete vulnerability scanning coverage

Ref.	Recommendation	Agreed Management Action	Owners/Contributors	Timeframe
1.1	1. A full review of the content of the Configuration Management Database (CMDB) should be performed to identify any Council technology assets (including critical IP	A monthly hardware asset management review is provided to the Council that is reasonably comprehensive and granular. This	**Owners:** Richard Carr, Interim Executive Director Corporate Services; and Mark Bulmer, Vice President Consulting Services, CGI	31/12/2023

	addresses for static devices) that are not included. 2. Ensure that missing assets are identified and the CMDB updated to include their details. 3. Establish processes to confirm the ongoing completeness of the population of CMDB assets. This should be linked to established asset addition and disposal processes.	will be updated to reflect the points noted above.	**Contributors:** Nicola Harvey, Service Director, Customer and Digital Services Heather Robb, Chief Digital Officer; Mike Brown, Cyber Security Manager, Digital Services Mark Burtenshaw, Cyber Security Officer, Digital Services Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	
1.2	The following controls should be implemented to confirm and provide assurance that ongoing vulnerability scanning covers the entire Council technology estate: 1. Agree a methodology or process between CGI and the Council to confirm that planned vulnerability scans include the Council's full network range prior to the start of the scanning process. 2. Perform ongoing reconciliations between the content of the Configuration Management Database (CMDB) and the technology assets to be included in scans to confirm that all expected assets are included.	Digital Services will liaise with CGI to agree processes and assurance arrangements aligned to the recommendations above. Internal Audit will be advised of the outcomes of the review and details of processes implemented provided.	**Owners:** Richard Carr, Interim Executive Director Corporate Services; and Mark Bulmer, Vice President Consulting Services, CGI **Contributors:** Nicola Harvey, Service Director, Customer and Digital Services Heather Robb, Chief Digital Officer; Mike Brown, Cyber Security Manager, Digital Services Mark Burtenshaw, Cyber Security Officer, Digital Services Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	31/12/2023

Finding 2 – Vulnerability Prioritisation and Remediation

Finding Rating	Medium Priority

Review of established vulnerability remediation processes confirmed that:

Vulnerability prioritisation - critical asset vulnerabilities are not prioritised for resolution as information on asset criticality is not currently available

Vulnerability remediation - critical or significant medium vulnerabilities are not currently patched within 48hrs of release of patches from system / software providers (for example Microsoft) as required per Schedule Part 2.4: "Security Management" of the established CGI contract.

Management has advised that that an informal agreement has been established between CGI and the Council to adopt a more practical remediation approach that is aligned with recommendations from authorised threat intelligence sources such as National Cyber Security Centre (NCSC), however no revised patch implementation timeframes have been specified, and this change has not been reflected in the contract.

Risks

- **Technology and information** - patches to address critical or significant medium vulnerabilities are not prioritised or applied in a timely manner, exposing the Council to a risk of a potential cyber-attack.
- **Supplier, contractor, and partnership management** – operational processes do not reflect established contractual requirements.

Recommendations and Management Action Plan – Vulnerability Prioritisation and Remediation

Ref.	Recommendation	Agreed Management Action	Owners/Contributors	Timeframe
2.1	1. A process should be established to identify and prioritise remediation of any critical assets where critical or significant medium vulnerabilities have been identified (ideally based on criticality assessments from the Configuration Management Database – refer recommendation 1.1). 2. Where the asset criticality has not been previously determined & documented, clarification in relation to their significance and prioritisation for remediation should be obtained from the Council.	For all P1 systems (where CGI hardware is deemed to be a critical asset), Digital Services will work with CGI to identify critical and high vulnerabilities on a quarterly basis and ensure that a remediation plan is prepared and put in place that prioritises critical assets. Risk acceptance of individual vulnerabilities may be required at times to ensure business continuity.	**Owners:** Richard Carr, Interim Executive Director Corporate Services; and Mark Bulmer, Vice President Consulting Services, CGI **Contributors:** Nicola Harvey, Service Director, Customer and Digital Services Heather Robb, Chief Digital Officer; Mike Brown, Cyber Security Manager, Digital Services	20/12/2024

			Mark Burtenshaw, Cyber Security Officer, Digital Services Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	
2.2	1. Refreshed timeframes for the patching of critical or significant medium vulnerabilities following release of patches from system / software providers should be agreed between CGI and the Council. 2. Schedule Part 2.4: “Security Management” of the established contract should be updated to reflect these refreshed timeframes, together with any relevant key performance indicator metrics	Digital Services will review the current CGI contract obligations and, if possible, make changes where relevant. Internal Audit will be advised of the outcomes of the review	**Owners:** Richard Carr, Interim Executive Director Corporate Services; and Mark Bulmer, Vice President Consulting Services, CGI **Contributors:** Nicola Harvey, Service Director, Customer and Digital Services Heather Robb, Chief Digital Officer; Mike Brown, Cyber Security Manager, Digital Services Mark Burtenshaw, Cyber Security Officer, Digital Services Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	30/06/2023

Finding 3 – Security policy exception management

Finding Rating	Medium Priority

CGI currently has no established formal exception tracking process that records approved vulnerability management (and other relevant) exceptions from established security policies and standards; and confirms that they are approved at an appropriate level and closed when exception timeframes have expired.

CGI management has confirmed that an informal process is applied where exception approvals are requested from the CEC Cyber Security Team and individually reviewed and approved via email by the CEC Cyber Security Manager.

To support ongoing vulnerability management, the following examples of exceptions may be required:

1. System Baseline Exceptions - operating system baselines (pre-configured settings (including security) applied to a system before it is released into production) are defined and gold (standard or master) images are used to support baseline deployment across various operating systems.

Gold images are secured with enhanced controls that are reviewed and approved by the Information Security team. However, some business or technical requirements may involve changes to images, which should be approved though an established exception process.

2. Patch schedule exceptions - there is a defined patching schedule for servers, and patching is performed in line with this schedule by system administrators. Again, some business or technical requirements may require exceptions to the defined patching schedule.

Risks

Technology and information

- If exception timeframes are not monitored and closed, vulnerabilities could remain in the system, resulting in increased security risks.
- Reviewing exception requests individually does not provide a view of the cumulative risks associated with multiple related and / or unique security policy exceptions.

Recommendations and Management Action Plan – Security policy exception management

Ref.	Recommendation	Agreed Management Action	Owners/Contributors	Timeframe
2.1	A comprehensive centralised security exception tracking process should be developed and implemented that captures relevant information associated with each request. This should include: 1. Centrally recording and maintaining the following information:	Digital Services will liaise with CGI to review existing process and documentation available for this and discuss how this can be changed within the existing contract.	**Owners:** Richard Carr, Interim Executive Director Corporate Services; and Mark Bulmer, Vice President Consulting Services, CGI **Contributors:**	30/09/2024

	• Nature of exception and relevant policy/standard/document that would normally apply. • Risk associated with the exception request • Exception significance based on risk (e.g., critical; high; medium; low) • Requestor • Reviewer/Approver, • Duration of exception • Responsibility for exception remediation / closure 2. The cumulative risks associated with all open exceptions should be considered and recorded when considering new exception requests. 3. Ongoing monitoring should be performed to confirm that cumulative risks associated with open exceptions remain within appetite, and that all exceptions have been remediated within agreed timeframes. 4. Open exceptions that have not been remediated / closed within agreed timeframes should be investigated and resolved.		Nicola Harvey, Service Director, Customer and Digital Services Heather Robb, Chief Digital Officer; Mike Brown, Cyber Security Manager, Digital Services Mark Burtenshaw, Cyber Security Officer, Digital Services Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Internal Audit Report

Fraud and Serious Organised Crime

26 September 2022

CW2009

Overall Assessment	**Significant Improvement Required**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Significant improvement required

Overall opinion and summary of findings

Significant control weaknesses were identified in both the design and effectiveness of the Council's fraud and serious organised crime (SOC) (including anti-money laundering (AML)) control environment and governance and risk management frameworks.

Consequently, only limited assurance can be provided that fraud and SOC risks are being identified and effectively managed, and that the Council's objectives of managing and mitigating the impacts of fraud and serious organised crime will be achieved.

Ongoing Assurance

Review of a sample of established first line service fraud management arrangements confirmed that (whilst inconsistent) they were generally well designed, although there is currently no ongoing service and directorate (first line) or established second line assurance performed to confirm their ongoing effectiveness.

A lack of ongoing assurance presents a challenge for individual directors and the Corporate Leadership Team (CLT) in meeting their responsibilities outlined in Council policies to ensure that the Council develops and maintains effective controls to detect and prevent fraud, bribery, and anti-money laundering.

The Council also has limited assurance that new controls are being designed and implemented to combat the pace and consistently changing nature of fraudulent activity.

It is acknowledged that this may be addressed by implementation of the planned governance and assurance model, and that external audit will provide some assurance on key financial controls during to support preparation of the financial statements.

Reporting

There is no established Council-wide process for recording fraud; SOC; and AML incidents, across Council services, or consolidated reporting provided to directorates and the CLT to provide a view on the volume; nature; and impact of frauds that occur. Consequently, the Council has no overarching view of the volume and impact (including the financial impact) of incidents and cannot clearly define whether and what action is required to improve the design and effectiveness of established fraud prevention and detection controls.

Whilst there is a clearly defined escalation route for fraud and SOC incidents defined in Council policies to the Chief Executive; Monitoring Officer; Money Laundering Reporting Officer; and Chief Internal Auditor; numbers reported are low.

This suggests either the volume; nature; and impact of fraud experienced across the Council is immaterial, or that fraudulent activity is potentially not being identified and escalated in line with established policy requirements.

Risk Management

Fraud and SOC is an enterprise risk for the Council, which is reviewed and assessed regularly at a Council wide level, however there is no established process in place to identify and manage thematic service fraud and SOC risks across the Council.

The Corporate Resilience team were advised through previous discussions with the Corporate Risk Team circa 2019, that consideration of fraud and SOC related risks should be performed within individual service areas as part of the Council's corporate risk management approach.

Phased Implementation Approach

It is recommended that a phased implementation approach is adopted, to enable sufficient time for the design and implementation of the new process. The new process should give consideration to Audit Scotland expectations as detailed in their July 2022 publication on Fraud and Irregularity.

Audit Assessment

Audit Areas	Findings	Priority Rating		Areas of good practice
1. Anti-Money Laundering Arrangements 2. Strategy and Governance 3. Training 4. Partnering 5. First line arrangements	1. Established Fraud and Serious Organised Crime Arrangements	**High Priority**		• Fraud prevention, Anti-bribery, and Anti-Money Laundering policies have been established and are published on the Council's intranet (the Orb). • The Council has established a Serious Organised Crime Group which includes a wide breadth of representation across the Council with external input (such as Police Scotland) as required. • The Council has a clearly defined risk appetite for fraud and SOC. • An annual fraud and detection report provides details on fraud detection and prevention activities undertaken by the Customer Fraud Team and outcomes of the NFI exercise. • Information sharing protocols in relation to Fraud and SOC are in place. • The Council participates in the Scottish Local Authority Investigators Group (SLAIG) and the Institute of Revenues Rating and Valuations (IRRV) professional group. • The services most likely to be impacted by fraud and SOC have established fraud prevention and detection processes. • There is a clearly defined fraud and SOC escalation route to the Council's Monitoring Officer; Chief Internal Auditor; and Chief Executive; and a clearly defined escalation rout to the Money Laundering Reporting Officer (MLRO), together with a requirement for provision of an annual money laundering report by the MLRO to the Governance, Risk, and Best Value Committee. • The Council's external website includes a link to an electronic fraud form enabling citizens and other parties to report a possible fraud. • Various training and awareness sessions for employees and elected members have been facilitated by the Corporate Resilience team.
	2. Risk Management – Fraud and SOC	**Medium Priority**		

Background and Scope

The Scottish Government's Serious Organised Crime Strategy outlines how Scotland should work together to reduce the harm caused by serious organised crime (SOC). The Strategy defines SOC as a crime that:

- involves more than one person
- is organised, involving a level of control, planning and specialist resources
- causes, or has the potential to cause, significant harm
- involves financial or other benefit to the individuals concerned

Local authorities (LAs) face significant risks related to fraudulent transactions and other criminal activities, including money laundering, perpetrated by SOC groups. Further areas of risk and vulnerability related to serious and organised crime include cybercrime, human trafficking, bogus tradespeople, inadvertent funding of SOC groups through procurement and licensing activities, counterfeit goods etc.

LAs can be used by criminals and anti-social elements to facilitate their money laundering activities.

Relevant Legislation and Guidance

Relevant fraud, Anti-Money Laundering (AML), and SOC legislation that applies to the Council includes:

- Criminal Justice and Licensing (Scotland) Act 2010
- Serious Crime Act 2007
- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017

Whilst LAs are not directly included within the scope of anti-money laundering legislation, the Chartered Institute of Public Finance and Accountancy (CIPFA) advises LAs to proactively comply with the underlying principles of the anti-money laundering legislation and regulations, and not to presume that money laundering isn't an issue for local government.

Consequently, CIPFA considers that it is good practice for LAs to appoint a designated Money Laundering Reporting Officer (MLRO) and apply AML policies and procedures.

LAs are also expected to play active part in the wider remit of the Scottish Government Serious Organised Crime Strategy through active cooperation with the wider network of partnering agencies, including provision of good quality data for the purpose of knowledge sharing / data matching exercises.

Covid-19 Impacts

Recent CIPFA and Audit Scotland publications have highlighted significantly increased fraud and SOC risks, as a result of the Covid-19 pandemic. These are primarily due to high amounts of funding distributed by public bodies; the need to respond quickly; relaxation of certain public contract procurement and grant approval requirements; and the impact of homeworking and physical distancing on routine validation and data security checks.

The Council's approach to Fraud and SOC

Key Council policies designed to ensure compliance with applicable legislation and manage the Council's potential fraud and SOC risks include:

- Fraud Prevention Policy
- Anti-Bribery Policy
- Whistleblowing Policy
- Employee Code of Conduct

The Council's Fraud and SOC Framework

The Council has no established second line framework that provides fraud and SOC guidance to directorates and services, and no centralised reporting and oversight of fraud and SOC incidents.

Each directorate and their services are responsible for identifying their relevant fraud and SOC risks and implementing appropriate processes; procedures; and controls to ensure that these risks are effectively managed and confirm alignment with the Council policies noted above. This will often involve working closely with multi agency partners (for example Police Scotland).

It is acknowledged that implementation of a framework would be complex given the volume and variation of fraud and SOC risks that could potentially impact a number of Council services, and the complex governance and oversight of these services and their associated risks performed by relevant executive committees.

Council Serious Organised Crime Group

The Council's SOC Group was established at the request of the Corporate Leadership Team (CLT) to coordinate and monitor the Council's fraud and SOC activities in response to Scotland's SOC Strategy. The Group is chaired by the Resilience Manager, who has delegated responsibility for the coordination of the Council's response to serious and organised crime including:

- raise awareness of potential vulnerability from SOC and other forms of corrupt practice
- enhance resilience against corrupt practice
- develop, agree and monitor the annual workplan
- share good practice
- ensure appropriate infrastructures and internal controls are in place

corporately promote the benefits of positive ethics and integrity.

The Council's SOC group meets quarterly and reports to the Edinburgh Multi-Agency Serious Organised Crime Board chaired by Police Scotland.

The Council's SOC group is also responsible for completion of the Local Authority Serious and Organised Crime Checklist provided by SOLACE. The checklist is designed to be used as an internal self-assessment tool by senior management to provide a high-level overview of the serious and organised crime risks that could potentially impact each authority.

Customer Fraud Team (CFT) and National Fraud Initiative

The Council's CFT investigates and recovers the proceeds from fraudulent activity reported by members of the public or other government agencies. This includes external fraud home visits.

The Council also participates in Audit Scotland's National Fraud Initiative (NFI) exercise, which is a comprehensive data matching exercise completed over a two-year period that compares information held by public bodies to highlight discrepancies between the records held across various public organisations and identify any potential instances of fraud.

An annual fraud and detection report is presented to the Finance and Resources Committee which provides details on fraud detection and prevention activities undertaken by the Customer Fraud Team and outcomes of the NFI exercise.

Scope

This review assessed the adequacy of the design of the governance arrangements and operational processes and controls established by directorates to support services with effective management of their fraud and serious organised crime risks, and established assurance arrangements to confirm that processes and controls are being consistently and effectively applied.

We also considered the processes established to support completion of the UK Government's local authority serious and organised crime checklist, and the adequacy and effectiveness of governance arrangements established to provide a holistic view of the management of fraud and SOC risks and incidents across the Council, with focus on the areas detailed below:

- Licensing
- Planning and Development Management
- Council housing allocations and end of tenancy agreements
- Finance and Procurement
- Customer and Digital Services (CFT and financial transaction processing)

Risks

The review also considers assurance in relation to the following Corporate Leadership Team (CLT) risk:

- Fraud and Serious Organised Crime

Limitations of Scope

This review was limited to assessing the design of the Council's established fraud and SOC governance and risk management processes and supporting policies; procedures; and controls but did not consider their effectiveness.

Whistleblowing was also specifically excluded from the scope of this review as this was considered by the separate independent review.

Reporting Date

Testing considered the period 2017 to 2022. Our audit work concluded on 20 September 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Established Fraud and Serious Organised Crime Arrangements

Finding Rating	High Priority

Review of the Council's Fraud and Serious Organised Crime (SOC) arrangements highlighted:

1. The Council does not have a clear fraud, SOC, and AML strategy and plan that covers both operational and cyber fraud.
2. The Council's fraud prevention policy is dated 2013. Review of the current policy confirmed that:
   - the policy refers to the Council's Monitoring Officer as having overall responsibility for the policy. This is incorrect and reflects historic structures where the Director of Corporate Governance (who was also the Council's Monitoring Officer) had overall policy responsibility and the Head of Finance, as one of their direct reports, was the policy owner. The references require updating to refer to the Director of Corporate Services.
   - it states that the Council's Internal Audit (IA) service plays an important role in the prevention and detection of Fraud. This suggests that IA has responsibility for ownership of key operational fraud prevention controls, which is incorrect and does not support IA independence. This reference is also included in the Anti-Money Laundering Policy.
   - it states that the Council's financial and non-financial systems are also independently monitored by Internal Audit. This suggests that Council systems are reviewed by IA on an ongoing basis, which is not aligned with the risk based annual IA plan and does not recognise the role of External Audit.
   - it does not provide detail on the significance of frauds (e.g. value and impact) that should be escalated to senior management.
3. The Council's anti-bribery policy is dated 2015. Review of this policy and the supporting anti-bribery procedure confirmed that they refer to historic risk management procedures, and risk management officers in directorates /services who are no longer in post.
4. Clearly defined fraud and SOC roles, responsibilities, and accountabilities for first line services and the second line framework owners and assurance teams have not been established. In addition, work is required to understand potential key-person dependencies to ensure there are adequate resources and deputising arrangements to for oversight during absence periods as required.

   It is acknowledged that the fraud prevention policy includes a generic statement that directors are responsible for the prevention and detection of fraud, the ant-bribery policy includes clearly defined responsibilities, and the Council's Response to Serious Organised Crime Group has responsibility to oversee compliance with Scotland's Serious Organised Crime Strategy.
5. Processes for consistent recording; collation; and reporting fraud and SOC incidents (including AML) across the Council with reports provided to senior management; directors; and the Corporate Leadership Team (CLT) on total incident volumes and their nature and impact (including financial losses) have not been established.
6. A system that supports ongoing recording of fraud; SOC; and AML incidents across Council services is not in place.
7. There is limited information available for services on how to mitigate; identify; manage; address; and report on fraud and SOC incidents.
8. There is limited ongoing assurance on the adequacy and effectiveness of specific fraud and SOC training developed by services and delivered to employees
9. Fraud and SOC e-learning is not reviewed regularly to reflect the changing external environment; the nature of new and emerging fraud and SOC risks; and AML awareness and reporting requirements.

10. Appropriate information and support for Council employees who could potentially suffer from intimidation, harassment, and internal and / or external pressure to engage in fraud and SOC activities has not been developed.
11. An Information Sharing Protocol relation to 'Data washing/Data Sharing' has been drafted and provided to Police Scotland, however feedback and finalisation is outstanding.
12. It is also noted that the Edinburgh Serious Organised Crime Multi-agency forum (a Police Scotland led group which the Council is a member of) has not met formally since August 2019, with no immediate plans to reinstate these meetings.

    The Corporate Resilience team have advised that this is a known issue across a number of local authorities and there have been several requests to the Scottish Government and Police to resume these meetings with no success.

Risks

The potential risks associated with our findings are:

- **Governance and Decision Making** - Fraud and SOC control weaknesses are not identified and addressed through assurance processes, and fraud and SOC incidents and potential incidents are not reported and managed appropriately, with no corporate view of the nature and impact of incidents impacting the Council.
- **Fraud and Serious Organised Crime** – lack of clarity across the Council on frauded and SOC roles, responsibilities, and accountabilities.
- **Workforce** – employees may not be adequately protected from intimidation, harassment, and internal and / or external pressure to engage in fraud and SOC activities.

Recommendations and Management Action Plan – Established Fraud and Serious Organised Crime Arrangements

Ref.	Recommendation	Agreed Management Action	Action owner, key contributors, and estimated date
1.1	The Council's fraud and SOC arrangements should be reviewed, this should include: • update of relevant policies and development of an overarching framework which gives consideration to the issues noted above and is aligned with Audit Scotland expectations on public body counter-fraud arrangements.	Fraud and SOC arrangements will be reviewed and appropriate recommendations for relevant policies and the framework presented to CLT for approval. The revised arrangements will give consideration to Audit Scotland expectations as detailed in their July 2022 publication on Fraud and Irregularity. A phased implementation approach will be adopted, to enable sufficient time for the design and implementation of the new process.	**Owner:** Richard Carr, Interim Executive Director of Corporate Services **Key Contributors:** Hugh Dunn, Service Director – Finance and Procurement Nick Smith, Service Director – Legal and Assurance Gavin King, Head of Democracy, Governance and Resilience

Ref.	Recommendation	Agreed Management Action	Action owner, key contributors, and estimated date
1.1 cont.	• agreement for where overall responsibility for the framework should sit. Given the current structure of Council and recognition that associated risks are largely related to financial impacts, overall ownership by Finance may be appropriate with support from Corporate Resilience, ultimately this is management's decision. • Formal agreement from Police Scotland on information sharing and future arrangements for the Edinburgh Multi-Agency Serious Organised Crime Board • It is also recommended that the framework is aligned to implementation of the planned Governance and Assurance model to ensure that appropriate and proportionate ongoing first and second line assurance is provided on fraud (including cyber fraud) and SOC high risk services that are most likely to be impacted.	An implementation plan that considers and addresses (where possible) the IA recommendations included in this report will be prepared by 31 March 2023. The plan will be agreed with all services and external stakeholders who will be required to support the process. The plan will be shared with Internal Audit to confirm that appropriate actions have been defined, or risks accepted (where appropriate), and management actions will then be agreed based on the content of the plan, with their implementation progress monitored through the established Internal Audit follow-up process.	Mary-Ellen Lang, Corporate Resilience Manager **Estimated date for completion of implementation plan**: 31 March 2023

Finding 2 – Risk Management – Fraud and SOC

Finding Rating	Medium Priority

Risk identification and reporting

The Council's current risk profile includes Fraud and SOC as a key risk category which is reviewed and reported to CLT and Committee. Whilst this includes consideration of high-level associated risks and impacts at a directorate level, there is no established process in place to identify; record; assess; escalate; and manage thematic service fraud and SOC risks across the Council. The Corporate Resilience team raised this through previous discussions with Corporate Risk Management (circa 2019) who advised that risk management work and recording of relevant risks should be performed within individual service areas.

Completion of the annual fraud and SOC checklist (produced by SOLACE, a consulting local government group) is the responsibility of the Council's SOC group and supports identification of thematic risks, however the checklist was last completed in full in July 2019. Management advised that work to update the checklist in commenced in July 2020, however it was not completed due to Covid-19.

It is acknowledged that implementation of the Council's refreshed risk management framework should enable production of consolidated risk reporting to inform the Corporate Leadership Team and Governance, Risk, and Best Value Committee on thematic fraud and SOC risks, and support comparison between the current fraud and SOC risk profile and the Council's agreed risk appetite. It does however remain the responsibility of services to ensure that relevant risks are recorded.

Risks

The potential risks associated with our findings are:

- **Governance and Decision Making** - The Council's fraud, SOC and AML risks are not effectively identified and managed.

Recommendations and Management Action Plan – Risk Management: Fraud and SOC

Ref.	Recommendation	Agreed Management Action	Action owner, key contributors, and estimated date
2.1	Development of the framework at recommendation 1.1 should include engagement with the corporate risk management team to ensure processes are established to identify; assess; and record thematic fraud; serious organised crime (SOC) and anti-money laundering (AML) risks across Council services. In addition, the annual SOLACE fraud and SOC checklist should be completed, and results reviewed by the Council's SOC group. Any gaps identified should be recorded in the CLT risk register, with mitigating actions and implementation timeframes agreed and implementation progress monitored.	As per 1.1, this will be addressed via the phased implementation approach and implementation plan.	**Owner:** Richard Carr, Interim Executive Director of Corporate Services **Key Contributors:** Hugh Dunn, Service Director – Finance and Procurement Nick Smith, Service Director – Legal and Assurance Gavin King, Head of Democracy, Governance and Resilience Mary-Ellen Lang, Corporate Resilience Manager **Estimated date for completion of implementation plan**: 31 March 2023

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Internal Audit Report

Employee Wellbeing

31 August 2022

CW2102

Overall Assessment	Some Improvement Required

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Some Improvement Required

Overall opinion and summary of findings

Whilst some control weaknesses were identified in the consistent application and effectiveness of established wellbeing processes and initiatives implemented across the Council during Covid-19, they provide reasonable assurance that employee wellbeing is being managed, and that the Council's 'Our People' objective to provide ongoing focus on the physical, mental, and emotional wellbeing of our employees should be achieved.

Audit outcomes

Survey responses identified three recurring themes, highlighting that respondents felt that messages from the Corporate Leadership Team are not consistently and effectively communicated across teams; that there were inconsistent approaches to employee wellbeing across the Council (most noticeably completion of display screen; risk; and stress risk assessments); and that employee capacity to deliver existing and future service demands has a significant impact on ability to focus on wellbeing.

It is important to ensure employee feedback is considered and addressed as the Council continues to face significant workforce challenges, including ongoing Covid and other sickness absences; retention and recruitment challenges; ongoing service delivery challenges as the Council continues to respond to Covid and other demands for support (for example the Ukraine crisis); and the extent of the change agenda that the Council is being asked to deliver.

Consequently, three medium rated findings have been raised together with recommendations for management to consider. Further information is included at Section 3.

Areas of good practice

- The Council introduced a Covid related absence scheme with full pay for colleagues absent with a Covid related reason. This was also extended beyond health/medical related instances to include those with caring responsibilities.
- A wide range of wellbeing activities and employee support is provided, including employee wellbeing roadshows delivered both remotely and across a range of services based in various geographic locations across the city.
- Wellbeing initiatives are effectively communicated to all employees with a Council email address, and to those who provided their own personal email addresses to receive Council communications.
- Communication of wellbeing initiatives to employees with no email address through use of payroll inserts.
- Sickness absence data is regularly reviewed to identify key themes with a dashboard and supporting commentary provided to both Directorate and the Corporate Leadership Teams.
- Remote working practices provide an improved ability to manage work/life balance for those able to work from home. Employees surveyed advised were able to plan their days more effectively, factoring in time for breaks, exercise and wellbeing activities.
- MS Teams is used for regular meetings, wellbeing checks and interactions with managers and has increased the ease of adapting to hybrid working.
- A number of respondents felt the council took the risks identified with coronavirus seriously and were quick to implement government guidelines on hand sanitising, face masks, and social distancing supporting employees with their physical wellbeing concerns.
- Covid-19 manager and employee guidance was developed; regularly updated; and published on the Orb (the Council's intranet).
- A new leadership goal has been introduced for 2022/23 onwards which signposts expectations of managers with associated measures for leading, developing and supporting teams.
- A new People Board has been established which should support ongoing focus on the design and implementation of employee wellbeing initiatives.

Audit Assessment

Audit Areas	Findings	Priority Rating
1. Human Resources employee wellbeing initiatives and guidance	1. Employee Communications	**Medium**
2. Employee wellbeing surveys	2. Varying approaches to wellbeing across the Council	**Medium**
3. Directorate and Service wellbeing activities	3. Capacity to Focus on Employee Wellbeing	**Medium**

Basis of opinion

Our audit opinion is based on the outcomes of discussions with employees and results of audit surveys completed by employees. A total of 205 responses were received. The majority of responses were from colleagues with people management responsibilities (176) with the remaining 29 front line or furloughed employees. Responses represent approximately 1.75% of employee roles most likely to have been impacted by Covid-19 (circa 11,600 in total) and 0.9% of the total number of Council employees.

There was limited attendance at a series of one hour working groups arranged to support the audit with only 6 first-line colleagues attending the sessions. It is acknowledged this could be attributable to the Council's wider engagement culture, as there has typically been limited engagement in previous Council-wide surveys and workshops.

Review of qualitative survey feedback highlights that increased workloads; potential survey fatigue; and lack of confidence in the Council's ability to effectively implement change could also be potential reasons for the limited attendance at workshops. There was also a low response rate from furloughed employees and those with no Council email addresses.

Further detail on our audit approach, sample selection, survey details and response rates is included at Appendix 2.

Qualitative feedback from employees

Qualitative comments were provided in survey responses which covered a wide range of themes. These have been collated and shared with senior management to highlight what worked well, and where further areas of improvement was indicated by survey respondents.

Background and Scope

Employee health and wellbeing is a core element of any People strategy, as investment in employee wellbeing should result in increased organisational resilience; better employee engagement; reduced sickness absence; and higher performance and productivity.

The City of Edinburgh Council's Wellbeing approach

The Council's Business Plan includes a section on 'Our People' that highlights the Council's ongoing focus on the physical, mental, and emotional wellbeing of employees as detailed in the Council's People Strategy 2021 - 2024 approved in April 2021. In addition, the Council's Wellbeing Strategy is an integrated strategy that was approved in 2019, with the objective of implementing a holistic approach to employee wellbeing.

Supporting resources and guidance for mental, physical and emotional health is available for both employees and managers, and a range of ongoing employee wellbeing roadshows that include sessions with internal and external experts on various physical and mental health topics have been provided.

Wellbeing surveys were completed in April and November 2020 with a 14% and 12% employee response rate that focused on employee wellbeing; caring responsibilities; working from home; and active travel.

The Council's digital learning platform myLearningHub also includes a Wellbeing Hub (launched in November 2021) that provides access to useful wellbeing information, resources and access to wellbeing session recordings.

A significant challenge in relation to employee wellbeing is ensuring that all initiatives are communicated to the circa 5,000 employees who currently have no Council email addresses. Whilst the myLearning Hub can be accessed from any device, permission is required to use personal email addresses to access the system.

Covid-19 wellbeing response

The Council implemented operational resilience arrangements to support the health, safety, and well-being of employees during Covid-19. These included remote working where possible; enhanced health and safety measures for front line employees; a Covid related absence scheme; and furloughing employees where services could not be delivered.

Detailed coronavirus guidance related to working from home, Covid absences, health & wellbeing tips, tools and resources (including details of employee assistance program – PAM assist) have been published for both employees and line managers on the Orb and the Council's external website.

Risk assessments

In addition to the wellbeing initiatives and surveys highlighted above, the Council's stress management policy recommends that managers should perform individual and team stress risk assessments to prevent and detect any potential employee or team stress risk.

Corporate Health and Safety also recommends that employees perform Display screen equipment risk assessment to ensure that employees' working practices are safe and healthy and any gaps can be addressed.

General guidance on risk assessments is also provided via the Risk Assessment Toolkit on the Orb.

Scope

The objective of this review was to assess the effectiveness of the key wellbeing initiatives and controls applied by the Council during Covid-19 to assess and support employee wellbeing.

Risks

- Health and Safety
- Workforce

Audit Approach

The original Internal Audit testing approach was to:

- identify roles across the Council most likely to have been significantly impacted by Covid-19 (mainly front-line workers).
- issue surveys to people managers and employees in these roles and all furloughed employees.
- hold twenty separate one hour focus groups with a sample of circa 400 employees and managers, including those with no Council e mail addresses.

Due to limited uptake on focus groups this approach was then revised with surveys issued to the IA sample of furloughed employees; employees in roles most significantly impacted by Covid-19 and meetings arranged (where possible) with employees with no Council e mail addresses.

Communication was included in Managers' News to encourage employees to complete the surveys and completion timeframes were extended in an effort to increase response rates.

Sample Selection

1. Total Council employees (per iTrent) - 22,724.
2. From this, a total of 11,597 roles across all Council directorates that were most likely to have been impacted by Covid-19 were identified.
3. A random sample of 400 employees were then selected to participate in surveys / focus groups. This included 46 colleagues with no Council e mail addresses.
4. As part of responses, colleagues were asked to confirm whether they had people management responsibilities (it is not currently possible to identify people managers from iTrent records).
5. All 420 furloughed employees were also surveyed.
6. Surveys were emailed to all employees with a Council email address asking them to support the audit, and reminders were also included in Managers News.
7. Line managers engaged with colleagues with no email addresses to arrange meetings with Internal Audit.
8. All surveys were anonymous.

Survey details and a summary of response rates is provided at Appendix 2.

Limitations of Scope

The following areas were excluded from scope:

- Provision of personal protective equipment (PPE) to Council employees was specifically excluded from the scope of this review as this was covered in the Procurement and Allocation of PPE review completed in October 2020.
- Whilst colleagues with no Council email addresses were included in scope, challenges with engaging a representative sample of this colleague population were acknowledged.

Reporting Date

Our audit work concluded on 10 June 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Employee Communications

Finding Rating	Medium Priority

Review of established communication processes and survey feedback on communicating details of the Council's wellbeing initiatives, and Covid manager guidance to people managers confirmed that:

1. Known challenges regarding communicating with Council employees (circa 4,000 employees in predominantly front-line roles) who do not have a Council email address, and had not provided their personal email addresses, impacted levels of knowledge and awareness of wellbeing initiatives resulting in a key dependency on effective line manager cascade.

   50% of the employees surveyed with no Council email account advised they were not aware of employee wellbeing initiatives.

2. 45% of Council people managers surveyed, confirmed they were aware of the two employee wellbeing surveys conducted by the Council during Covid and had communicated the outcomes of the survey to their teams.

3. Wider Leadership Team (WLT) members would have been aware of the surveys and should have understood the need to cascade the request to complete them, and share the outcomes with their teams, therefore, the lack of people manager awareness suggests issues with communication from heads of service to their teams, most notably front-line employees with no Council e mail addresses.

4. The internal audit sample selection process also highlighted that some of the information held on the Global Address List (GAL) in relation to employee roles and reporting lines is out of date and requires updating. It is acknowledged that this could be due to the ongoing organisation restructure.

Risks

- **Workforce** - communication challenges could potentially impact the Council's ability to attract and retain talent in the current employment market
- **Service delivery** - performance and quality could be impacted if communication across all Council employees is not effective.

Recommendations and Management Action Plan – Employee Communications

Ref.	Recommendation	Management Response	Timeframe
1.1	Management should consider further ways to communicate with employees with limited system access. One option is feasibility of establishing securely hosted external web pages linked to the Council's website and can be accessed by	Use of hosted external web pages (extranet) have been used and are in place which contain certain information. As this requires information to be duplicated from the intranet this has resource implications to continue to do this ie. we are not resourced to do so. It is also not always appropriate to post certain documentation on an extranet.	N/A

	employees via secure log-in details. Should this be feasible, then all employee news and communications (including details of planned wellbeing initiatives and future wellbeing survey outcomes) should be published via these secure pages, with access rates monitored to determine the effectiveness of this communication channel.	All-employee access to the HR system is a current priority (for core system self-service) but this won't solve the issue of access to the Orb. Therefore, potential solutions for all employee access to the Orb is being explored through a Change request to CGI, (the Council's technology partner). Neither of these pieces of work will solve the issue of all employee access to Mylearninghub (unless personal email addresses are supplied – see below). Therefore, the risk is accepted at this time. In the interim, we are continuing our campaign to encourage employees who don't have access to our digital systems to sign up to receive direct communications to their personal email address. Once signed up they can receive Council wide communications, a weekly summary of Newsbeat articles, emergency notifications, as well as access to online learning and secure payslips.			
Ref.	**Recommendation**	**Agreed Management Action**	**Action Owner**	**Contributors**	**Timeframe**
1.2	a) The Wider Leadership Team should consider options for ensuring key messages, goals and priorities are cascaded across services and teams including opportunities to discuss in further detail where required. b) Management should consider options for automating updates to the Global Address List (GAL), for example via the iTrent system to support effective ongoing communications across the Council. If automatic updates are not possible, then regular reminders should be issued to employees to request information remains complete and accurate.	a) We will consider options for improving the communication and cascading of key messages; goals and priorities including options to update essential learning for managers and targeted communications via Managers' News. b) It is not possible to fully automate updates to the Global Address List (GAL) due to known limitations with linking iTrent and the GAL. A link to request updates to incorrect or missing details is provided via GAL entry for each employee. This request is then actioned by Digital Services colleagues, typically within 24 hours. In addition, regular reminders are issued by directorates to request that employees review and update their details as required. A further reminder will be issued to all employees reminding them to ensure their information remains up to date.	Richard Carr, Interim Executive Director of Corporate Services	Michael Pinkerton, Head of Communications Paul Lawrence, Executive Director of Place Amanda Hatton, Executive Director of Children's Services Judith Proctor, Chief Officer Edinburgh Health and Social Care Partnership	30/11/2022

Finding 2 – Varying approaches to wellbeing across the Council

Finding Rating	Medium Priority

It is acknowledged that ensuring full and effective support employee wellbeing was challenging at the beginning of the pandemic with managers adapting to the impact of Covid on their own wellbeing, whilst continuing to deliver critical services and managing workforce challenges where employees were impacted by Covid including shielding.

Survey responses and employee discussions highlighted varying approaches to employee wellbeing were applied across the Council. Specifically:

1. Of the population of employees and people managers who responded:

- 49% felt supported
- 35% did not feel supported
- 16% felt neither supported nor not supported

2. Completion of display screen equipment (DSE) assessments; provision of equipment for employees working from home; and completion of risk assessments for front line employees surveyed varied with:

- 49% of respondents who worked from home completed DSE assessments, and of that 49% some 47% advised that were provided with the correct equipment.
- Survey comments included mention of ‘lack of equipment’; ‘had to buy own equipment’; ‘lack of IT equipment/support’; ‘not provided with equipment’; and four specific comments stating that employee health was impacted due to incorrect equipment.
- Only 47% of managers surveyed confirmed they had completed risk assessments for front line employees delivering services during the pandemic.
- Employee survey respondents felt that some risk assessments ‘did not ask the right questions’; and some ‘risk assessments were not adhered to’. Comments also highlighted that some employees were adversely impacted physically and mentally from changes in workload; working patterns; and manager’s expectations.

3. Survey results note a gap between manager and employee views on the adequacy of ongoing employee wellbeing checks with:

- 99% of line managers who responded advising that they made contact with individuals and teams, with 13% saying they made contact monthly, 47% weekly, 17% daily, and 22% on an ad hoc basis.
- Almost all managers who responded advised they had been in contact with their team to carry out wellbeing checks.
- In contrast, 66% of general employees who responded (including those furloughed and those with no email address) confirmed that they received manager contact during the pandemic. In addition, survey feedback suggests a gap in perception of wellbeing checks between managers and their teams.
- 66% of employees who responded advised that they felt able to contact their managers with any wellbeing concerns.
- A number of respondents highlighted the impact of increased workloads and lack of manager support on their wellbeing, suggesting that whilst wellbeing concerns could be raised, they were not always addressed.

It should be noted that it was not possible determine thematic wellbeing outcomes across services and directorates as all survey responses were anonymous.

Risks

- **Workforce** – an inconsistent approach to wellbeing could impact the Council’s ability to engage, support, and retain employees.
- **Regulatory Compliance** – non-compliance with Health and Safety Executive requirements to complete DSE assessments and to complete and action risk assessments appropriately.

Recommendations and Management Action Plan – Varying approaches to wellbeing across the Council

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
2.1a	Communications should be issued to remind all employees and managers of the importance of completing DSE self-assessments. This should include links to guidance on the Orb, e-learning and details of employee and manager responsibilities, including ordering equipment (where required).	A communication will be issued to remind employees and managers of the importance of completing DSE self-assessments with links to current guidance and e-learning. In addition, Corporate Health and Safety will review the current guidance to ensure it reflects both the home working environment and the workplace, and other types of DSE equipment in use (e.g., tablets, and mobile phones).	Richard Carr, Interim Executive Director of Corporate Services	Chris Lawson, Head of Corporate Health and Safety Mike Pinkerton, Head of Communications	31/03/2023
b)	Communications should be issued to raise awareness of the Council's Stress Management Policy, Stress Management User Guide, and the supporting individual and stress risk assessments templates available via the Orb. In addition, managers should be reminded of their responsibilities to regularly complete and review the outcomes of both team and individual stress risk assessments and where required, develop an action plan to address concerns raised.	Communications will be issued to raise awareness of the Council's Stress Management Policy and user guide, including a reminder to managers to complete regular stress risk assessments, and take actions to address concerns raised.	Richard Carr, Interim Executive Director of Corporate Services	Katy Miller, Service Director Human Resources Mike Pinkerton, Head of Communications	30/11/2022
c)	Communications should be issued to remind managers to regularly review risk assessment templates and processes in line with the Risk Assessment Toolkit available via the Orb, to ensure they remain	A targeted communication was issued by Corporate Health and Safety via Newsbeat in August 2020, reminding all services including the Health and Social Care Partnership to review existing risk assessments and procedures to ensure they remain valid,	Richard Carr, Interim Executive Director of Corporate Services	Chris Lawson, Head of Corporate Health and Safety	30/11/2022

	appropriate for the services provided and work activities performed by their team. In addition, managers should be reminded to regularly review risk assessments (at least annually) and where required, reperform these to ensure they reflect current working practices and risks	accurate and appropriate and where required to complete new risk assessments. A further reminder will be issued with links to relevant guidance and advising further support and information is available from Corporate Health and Safety.		Mike Pinkerton, Head of Communications	
d)	Management should consider providing consolidated DSE, risk and stress risk assessment completion data and thematic outcomes to the Council's Health and Safety Group and directorate risk committees for review and resolution of any significant gaps.	Corporate Health and Safety will explore whether DSE and risk assessment workflows can be recorded and managed through the SHE system for reporting to management and trade unions as appropriate.	Richard Carr, Interim Executive Director of Corporate Services	Chris Lawson, Head of Corporate Health and Safety	31/03/2023
2.2	During audit discussions, some colleagues suggested having informal mental health wellbeing drop-in sessions held at various locations for colleagues with no Council email addresses. The Council should consider feasibility of providing this type of support.	The proposal for drop-in sessions would require fully trained/experienced individuals, and experience has shown that initiatives, such as the coaching bank, have little uptake in practice. Further support will however be provided on an ongoing basis through: • Promotion of Employee Assistance Plan/Occupational Health. • Continued provision of wellbeing roadshows with a range of topics available remotely and across different locations and at range of times. • Continued campaigning to encourage relevant employees to sign up for employee updates via personal email addresses so they can access Council wide communications, Newsbeat articles and e-learning. Communications regarding completion of ongoing employee wellbeing checks will be issued via Managers' News.	Richard Carr, Interim Executive Director of Corporate Services	Katy Miller, Service Director Human Resources Mike Pinkerton, Head of Communications	30/11/2022

Finding 3 – Capacity to Focus on Employee Wellbeing

Finding Rating	Medium Priority

Survey responses from people managers and employees highlighted that capacity challenges can provide limited opportunity to focus on wellbeing and attend wellbeing initiatives, and there is a gap between manager and employee views on the adequacy of ongoing capacity planning and workload management which is impacting employee wellbeing. Specifically:

- 75% of employees who responded advised that they were not actively encouraged to use time in their working day to focus on wellbeing.
- In contrast 91% of managers who responded advised that they had highlighted wellbeing initiatives to their teams.
- 58% of managers who responded felt they were encouraged to access or were able to access wellbeing initiatives.
- 67% of furloughed employees who responded advised they were encouraged to access wellbeing initiatives during their furlough time.
- 45% of employees who responded advised that their workload is not routinely monitored or reviewed.
- In contrast, 87% of managers who responded, advised that they monitor team workloads. The survey did not request details of the tools currently used across the Council to monitor workload.

Additionally, whilst furloughed employees who responded felt that they were well supported during furlough, some highlighted limited focus on their wellbeing following their return to work.

Risks

- **Health and Safety (employee health and wellbeing) –** employees are exposed to conditions or situations that harm their health and wellbeing, including stress and trauma.
- **Workforce planning** – existing workforce capacity does not meet the requirements to deliver strategy, services, and projects; and inability to attract and retain talent.
- **Strategic delivery –** the Council may be unable to deliver the objectives of the Strategic Workforce Plan 2021 - 2024.

Recommendations and Management Action Plan – Capacity to Focus on Employee Wellbeing

Ref.	Recommendation	Management Response	Timeframe
3.1	The Corporate Leadership Team (CLT) should consider options to enable colleagues to have sufficient time in their working days to focus on their wellbeing including attending wellbeing sessions where desired, while balancing delivery of critical services and Council priorities.	Ensuring all colleagues have access to and sufficient capacity to focus on wellbeing including participation in wellbeing activities is a key priority. Enabling this is linked to the planned review of the Council Business Plan, development of a medium-term financial plan and service delivery plans to support delivery of priorities. This will be risk accepted at this time and considered as part of a planned audit of workforce capacity in 2023/24.	N/A

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Appendix 2 - Survey Details and Response Rates

Sample details

Directorate	Sample Base	% Sample Base	Total Surveyed
Corporate Services	650	6%	22
Place	2,375	20%	82
Education and Children's Services	7,186	62%	248
Health and Social Care Partnership	1,386	12%	48
Employees surveyed	**11,597**	**100%**	**400**
Furloughed employees surveyed	**420**	**100%**	**420**
Total sample base	**12,017**	**-**	**820**
% Of roles most significantly impacted by Covid (sample base)	11,597	-	6.8%
% Of total Council employees	22,724	-	3.6%

Response Rates

Category of employees	Population Surveyed	Number of Responses	Response Rate
Furloughed Employees	420	3	0.7%
Meetings with employees with no email addresses	46	6	4%
Employees	154	20	13%
Managers	1000+*	176	18%
Total Responses	**205**		
% Of roles most impacted by Covid (excluding furloughed employees)	11,597	202	1.75%
% Of total employees (including furloughed employees)	22,724	205	0.9%

* Manager survey was across Council and was in addition to employee sample

Internal Audit Report

CGI Performance Reporting

14 September 2022

CS2103

Overall Assessment	Some improvement required

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Some Improvement Required

Overall opinion and summary of findings

Whilst some moderate and minor control weaknesses were identified in both the design of key performance indicators (KPIs) used to measure and report on CGI performance and operational performance controls, reasonable assurance can be provided that CGI's performance risks are being managed, and that the Council's objectives of confirming ongoing supplier performance effectiveness should be achieved.

Our review identified the need for CGI to improve some key operating controls to enable timely identification of instances where either Council networks or applications are not available and confirm that availability of the full population of applications is monitored in line with contractual requirements.

We also noted the need for both CGI and the Council to document and consistently apply the process supporting review of performance information prepared by CGI and provided to the Council.

Consequently, two medium and one low rated findings have been raised as detailed in section 3 below.

Audit Assessment

Audit Areas	Findings	Priority Rating
Governance	1. Network Availability	**Medium**
Performance Reporting Process	2. Application Availability	**Medium**
Issue management	3. Performance reporting review process – CGI and Digital Services	**Low**

Areas of good practice
The following areas of good practice were identified: • **Service Review Meetings** – a regular meetings have been established where KPI performance reporting is discussed, and actions taken and tracked to resolution. • **Incident Management** – incidents relating to the production or reporting of KPI performance reporting were managed through a process that is integrated into the wider incident management process.

Background and Scope

Third party performance reporting provides the Council with a means to gain oversight and assurance over activities performed by its partners and suppliers, to ensure that services are being provided in line with contractual requirements. As these services are critical to the overall operations of the Council, and failure to meet these requirements often carries a financial penalty, it is crucial that management information (MI) underpinning the performance reporting is complete and accurate.

Effective production of MI for performance reporting depends on a mature control environment that would typically include:

- effective governance structures, including defined reporting and escalation routes;
- a robust and well documented contract agreed with all parties;
- detailed performance reporting procedures;
- controls in place to review and reconcile data produced; and
- a robust issue management process to address any identified concerns by clients or stakeholders.

It is also important that the MI is shared with the appropriate people, who understand the data and how it relates to service levels/contractual requirements as well as how it impacts on the wider organisational risk.

CGI Performance reporting at the Council

The Council currently receives performance reports from its technology partner CGI, monthly, as part of the monthly service review meetings. A reporting pack is produced and sent to the Council on the fifth working day of the month, with the service review meeting held prior to the tenth working day of the month where this data is reviewed.

This pack contains the management information relating to all the KPIs contained within the CGI contract with the Council and is the primary method by which this information is produced and shared.

In addition, updates are provided relating to actions that are on the service review action tracker, as needed.

Scope

The objective of this review was to assess the adequacy and effectiveness of controls established to ensure completeness and accuracy of CGI reporting data and confirm that appropriate governance and issue management is in place to provide oversight over the CGI reporting process.

This review was performed by exercising the ‘right to audit’ clause included in the CGI contract.

Risks

The main risks associated with these findings is that it is not currently possible to confirm whether network and application availability service levels specified by the Council are being consistently achieved.

Additionally, potential inaccuracies in CGI performance data may not be identified and resolved, with associated performance service credits received and paid.

Limitations of Scope

The scope of our review was limited to the production of CGI performance reporting and oversight of the performance reporting pack performed by the Council.

The supplier management processes applied when KPIs have not been achieved were specifically excluded from scope.

Reporting Date

Our audit work concluded on 27 April 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Network Availability

Finding Rating	Medium Priority

Key Performance Indicators (KPIs) 17 – 22 in the KPI annex included in the established CGI contract relate to network availability, with specific focus on the time required to restore network services from the point of unavailability for each site. For example, if a site becomes unavailable at 6:02pm and is restored at 7:15pm, the length of unavailability is 1 hour and 13 minutes.

To ensure accurate reporting on network availability, CGI has established automated monitoring that monitors real time network performance and automatically creates alerts and / or tickets in the Remedy ticketing system when specific network availability events occur.

CGI currently measures network downtime from the time recorded on Remedy tickets; however, this approach will only be effective if the automated network monitoring process and the link with the Remedy ticketing system continue to operate effectively.

Review of this process established that:

1. **Automated monitoring control design and effectiveness** – CGI was unable to provide evidence of the design (for example design documentation) and ongoing assurance in relation to the effectiveness (for example outcomes of recent testing or reviews) of the established automated monitoring control, and its links to the Remedy ticketing system.
2. **Availability of logs from source systems** - Logs from source network devices could not be provided to enable validation / reconciliation of the time when networks became unavailable, and the time recorded on Remedy.
3. **Sample testing** – a review of three instances of network unavailability in the last 6 months highlighted that one Remedy ticket was raised manually. Whilst the ticket was correct, CGI could not provide a clear explanation for this exception to the automated process.

Risks

The potential risks associated with our findings are:

- **Technology and information** – network availability events are not identified and resolved in a timely manner if the automated monitoring control is not designed and / or does not operate effectively

Recommendations and Management Action Plan – Network Availability

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
1.1	The Council should request that CGI management: 1. Documents the design of the automated network monitoring process and its links to the Remedy ticketing system.	1. Risk accepted - CGI has confirmed that they will be unable to share the documented design of the network documented design of the automated network monitoring process and its links to the Remedy system as it used	Richard Carr, Interim Executive Director Corporate Services	Pete Scott, CGI Service Delivery Manager Nicola Harvey, Service Director,	30/10/2023

	2. Implements ongoing assurance / system testing to confirm that both processes are operating effectively as designed, with assurance outcomes recorded. This could include (for example) a reconciliation between availability incident timeframes recorded on source network devices and times recorded on the Remedy ticketing system. 3. Investigates and resolves any issues where linkages between the automated network monitoring process and the Remedy ticketing system have not operated as designed, resulting in manual Remedy tickets, and highlight them in performance reports provided to the Council. 4. Record the rationale for manually raised Remedy tickets that record network availability events and include details in the performance reports provided to the Council.	across all client accounts managed by CGI in the UK. 2. Risk accepted – CGI has confirmed that they are unable to provide assurance to the Council on the linkages between the automated network monitoring process and the Remedy ticketing system as this is not required per the terms of the current contract. 3. Manual Remedy tickets and their supporting rationale will be recorded in Client Service Reports provided to the Council.	Mark Bulmer, Vice President Consulting Services, CGI.	Customer and Digital Services Heather Robb, Chief Digital Officer Richard Burgess, Relations and Service Manager, Digital Services Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	

Finding 2 – Application Availability

Finding Rating	Medium Priority

KPIs 5, 6 and 7 in the KPI annex included in the established CGI contract relate to application availability for the Council's 86 priority 1, 2, and 3 (P1, P2 and P3) applications. Of these, 20 have been assessed as P1 (critical) applications.

The KPIs require application availability at either 99.5% or 99.9% over the monthly period, depending on the application priority level, and specify that application availability should be measured every 15 minutes (during the required uptime period – i.e., 24/7 for some applications and 8-8 for others).

Review of this process established that:

1. Completeness of ongoing availability monitoring - availability of only 19 of the 86 applications is currently monitored, including only 11 of the 20 P1 applications.
   Issues with availability for the remaining 67 applications (including 9 P1 applications) would only be identified if end users escalate the issue through the CGI helpdesk.
2. Applications maintained by CGI - applications managed by CGI are based on Council specifications. Consequently, where monitoring is not consistently included as part of the requirements, monitoring is not built into management of those applications, as doing so would incur additional costs.
3. Monitoring frequency – for applications currently monitored, availability is measured once per day, which is not aligned with the 15 minutes contractual requirement and is insufficient to confirm that monthly availability targets (99.5% and 99.9%) are being achieved.
4. Additionally, established KPIs (99.5% and 99.9% availability) mean that 24 x 7 applications can only be unavailable for approximately 45 minutes over the course of a month, and even less where application availability requirements are shorter (e.g., availability between 7am and 7pm).KPI measurement - CGI is not currently measuring application availability when it is reporting on KPIs 5 – 7.

   Instead, applications are treated as available until a ticket is raised highlighting that the application is not available. Unavailable time is recorded from the time the ticket was raised until it is resolved and used to calculate overall availability.

   As the KPIs are designed to measure overall availability and not the response time to a ticket being raised, or time taken to restore service, CGIs current method of reporting on this KPI based on when a ticket is raised and resolved may be incorrect.

Risks

The potential risks associated with our findings are:

Technology and information

- application availability issues are not identified and resolved in a timely manner if the full population of applications is not consistently monitored

Supplier, contractor, and partnership management

- established key performance indicators are not realistic and achievable
- unclaimed service credits due to misreporting of KPI performance data

Recommendations and Management Action Plan – Application Availability

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
2.1	The Council should request that CGI management: Investigates the feasibility of implementing automated application availability monitoring across the full population (86) priority 1, 2, and 3 applications used across the Council, or at least across the full population of 20 P1 (critical applications) at 15 min intervals in line with agreed contractual requirements. 1. Where this is feasible, implements a contractual change to support implementation of ongoing application availability monitoring across the population of the Council applications. 2. Includes ongoing application monitoring as a key element of standard build for all (or at least P1) future applications designed by CGI.	To be actioned as per recommendation.	Richard Carr, Interim Executive Director Corporate Services Mark Bulmer, Vice President Consulting Services, CGI.	Pete Scott, CGI Service Delivery Manage Nicola Harvey, Service Director, Customer and Digital Services Heather Robb, Chief Digital Officer; Richard Burgess, Relations and Service Manager, Digital Services	31/03/2023
2.2	It is recommended that Digital Services Management: 1. Reviews the appropriateness of established application availability key performance indicator (KPI) targets 5, 6 and 7 with CGI. 2. Requests that CGI investigates and implements (where feasible) alternative options for accurately identifying and recording application availability.	To be actioned as per recommendation.		Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	31/03/2023

Finding 3 – Performance reporting review process – CGI and Digital Services

Finding Rating	Low Priority

Review of the process established to support performance reporting established that:

1. The process applied by CGI to prepare performance reporting information covers creation of the performance reporting pack but does not currently detail the review process to be applied prior to finalising the pack and sharing it with the Council.
2. The process applied by the Council to review and approve performance reports has not been documented. Digital Services management has advised that this is currently being developed.
3. There is no assurance provided by CGI to the Council to confirm that the CGI performance reporting process remains appropriate; that performance reports are complete and accurate; and that both processes effectively support confirmation of ongoing delivery of contractual requirements.

Management has advised that currently, any concerns would be highlighted and resolved through established service review meetings.

Risks

Supplier, contractor, and partnership management

- risk that inconsistent review processes adopted by both the Council and CGI do not identify inaccuracies in performance reports

Recommendations and Management Action Plan – Performance reporting review process – CGI and Digital Services

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
3.1	CGI management should define and document the process for review of performance reports to be provided to the Council to confirm their completeness and accuracy.	The high-level process detailing CGI's internal review timeframes for monthly review of client service reports by the service delivery manager and final sign off by the head of service prior to issue has been added to the client service report creation document, and a screenshot of the timeline provided to Internal Audit.	Richard Carr, Interim Executive Director Corporate Services Mark Bulmer, Vice President	Pete Scott, CGI Service Delivery Manager Nicola Harvey, Service Director, Customer and Digital Services	Now closed

3.2	Digital Services management should: • Finalise the processes currently being documented to support review and approve CGI performance reports and ensure that this is consistently applied. • Implement an annual process to obtain assurance from CGI that the performance reporting process remains appropriate; the content of performance reports complete and accurate; and that both processes effectively support confirmation of ongoing delivery of contractual requirements. It is recommended that this assurance is based on testing performed by CGI, with details of the work performed, and outcomes provided to Digital Services.	The first bullet point of the recommendation will be delivered as per recommendation. Delivery of the second bullet point will be dependent upon CGI being able to perform the testing as anticipated by IA.	Consulting Services, CGI.	Heather Robb, Chief Digital Officer Richard Burgess, Relations and Service Manager, Digital Services Jackie Galloway, Commercial Manager, Digital Services Alison Roarty, Commercial Lead, Digital Services	31/03/2023

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Internal Audit Report

Management and Allocation of Covid-19 Grant Funding

CW2104

24 May 2022

Overall Assessment	**Effective**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Effective

Overall opinion and summary of findings

The control environment established to support the management and allocation of Covid-19 grant funding by the Council has been adequately designed, is operating effectively, and was consistently applied across both the discretionary business and taxi and private hire grant applications received.

This provides assurance that the Council's objectives of allocating Scottish Government funds to businesses in a timely manner, with minimum instances of fraud, have been achieved.

Our opinion is based only on a sample of discretionary business and taxi and private hire grants, as we were unable to review a sample of the 46,896 for Support for Business grants processed by the Council due to ongoing workforce and capacity challenges within Customer Services teams.

Whilst some moderate areas for improvement were identified in the grant management and allocation process for both the discretionary business and taxi and private hire grants, the potential risks that could have occurred were within management's risk appetite given the urgent need to disburse grant payments.

Consequently, one medium rated finding has been raised with the recommendation that the moderate control gaps identified are included in the Council's Covid-19 lessons learned assessment.

The audit assessment, areas of audit focus and good practice are detailed on page 4.

Audit Scotland's (Scotland's economy; Supporting businesses through the Covid-19 pandemic) report published in March 2022, notes that the Scottish Government placed reliance on councils' existing control environments and fraud arrangements, and relied on councils to ensure applicant eligibility.

The report also confirms that the Government has subsequently worked to assess fraud risks across the various support funds with work to detect fraudulent claims ongoing but estimates fraud and error in these schemes to be no more than one to two per cent of payments.

The outcomes of our review (whilst limited to only Discretionary Business and Taxi and Private Hire grants) confirm that the Council's grant allocation and management processes were applied in line with Scottish Government expectations. This should be validated by the outcomes of the next National Fraud Initiative data matching exercise (due November 2022) which will include business support funding payments

Additionally, the Government is retrospectively assessing how business support funding addressed equalities and supported specific demographic groups.

Audit Assessment

Findings summary	1. Grant Evaluation Processes	Priority Rating	Medium

Areas of audit focus	Areas of good practice
1. Grant evaluation and decision making	• There are clear guidelines for assessors to evaluate both grants in the form of a guidance sheet and logical process steps included in spreadsheets to support the assessment. • For discretionary business grants, new assessors recruited to support the process were paired with buddies. • For discretionary business grants, grant decisions were re-evaluated where information was received following payment (for example, confirmation that the applicant had received another Covid grant), resulting in a small number of reclaims. No instances were identified where management had not attempted to retrieve funding where further information was provided. • For both grants, there was clear segregation of duty with regards to grant payment, with payment requests independently checked prior to sending to the banking team. • For both grants, there was a short turn around between application, approval, and payment. • Correspondence with applicants on any issues with the initial application were clear and precise.
2. Rejections and appeals	
3. Grant Disbursement	
4. Citizen Engagement and Communication	
5. Secure document transfer and retention	
6. Oversight and Quality Assurance	
7. Management Information and Reporting	

Background and Scope

The Covid-19 pandemic resulted in the Scottish Government (SG) implementing two 'lockdowns'; new legislation; and a number of other restrictions to manage the spread of the virus that had a significant economic impact on the national and local economy and businesses.

Recognising the impacts of these restrictions on businesses, various tranches of SG funding were provided to local authorities who were requested to either allocate these funds in line with high level SG guidance, or to design an appropriate grant allocation process where no specific SG guidance was provided.

The Council was responsible for the urgent management and allocation of the following grant funding received from the SG, with the objective of mitigating short term financial challenges experienced by businesses that were adversely impacted by both lockdowns and other Covid-19 restrictions:

- **£12.3M Discretionary business grants** – the discretionary business grants process was designed and applied by the Business Growth & Inclusion team in Place.
- **£17.6M Taxi and private hire grants** – the process was designed by the Regulatory Services team within Place in line with published SG guidelines.
- **£260M Support for business grants** – the process was designed and implemented by the Customer Services team within Corporate Services who were required to develop different processes for the various scheme and iterations.

The design of each of the initial processes was reviewed by Internal Audit prior to their implementation, with feedback provided to management where opportunities to improve controls supporting administration of the grant were identified. It is acknowledged that grant allocation processes continued to evolve and change in line with SG guidance and reporting requirements.

It is expected that both the Scottish Government and external audit will request future assurance from the Council that the grant funding provided was effectively managed and allocated.

The total volume of applications awarded for each of the grants was:

- 5,960 for Discretionary business grants
- 4,398 for Taxi and private hire
- 46,896 for Support for business

Scope

This review assessed the effectiveness of the management and allocation of Covid-19 grant funding across the Council; confirmed that the processes designed were consistently applied; and that appropriate and proportionate checks were performed to identify any potential instances of fraud.

The review also provided assurance on the following Corporate Leadership Team (CLT) risks:

- Governance and Decision Making
- Service Delivery
- Regulatory and Legislative Compliance
- Reputational Risk
- Fraud and Serious Organised Crime

Limitations of Scope

The scope of this review was limited to confirming that the grant allocation processes were consistently and effectively applied, as the grant allocation process design was reviewed by Internal Audit prior to implementation.

Additionally, we were unable to review a sample of the 46,896 Support for Business grants processed by the Council due to ongoing workforce and capacity challenges within the Customer Services teams.

Reporting Date

Testing covered the period March 2020 to December 2021.

Our audit work concluded on 28 March 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Recommendations

Finding 1 – Grant Evaluation Processes

Finding Rating	Medium Priority

Review of a sample of 75 grant discretionary business grants and 65 taxi and private hire grants established the following:

1. **Minor grant evaluation inconsistencies**
   - two discretionary business grants had not been consistently evaluated. One applicant was rejected due to being unable to show a drop in income, whilst another was approved even though the applicant did not experience a drop in income.
   - one instance was identified with taxi and private hire grants; and one with discretionary business grants where information on bank statements did not match details included in the application form.
   - three instances were identified for taxi and private hire grants where the licence reference included in the application did not match Council records.
   - one discretionary business grant sample was identified where the address detailed on the application did not match the proof of address provided.
2. **Unclear guidance on business transactions (discretionary business grants)**
   - where no business bank statement were available, personal bank statements were accepted.

Assessors then reviewed the personal statement to identify business transactions to confirm existence of the business. Limited guidance was available to support this process, with reliance on professional judgement.

3. **Records retention**
   - for six discretionary business and one taxi and private hire grant files, e mail approval and rejections were not retained

Risks

Whilst these potential risks could have occurred, they were within management's risk appetite given the urgent need to disburse grant payments.

- **Financial and Budget Management** – the Scottish Government could potentially seek recompense from the Council for payments where applications have been assessed incorrectly.
- **Fraud and Serious Organised Crime** – inability to identify duplicate applications if details of approvals and rejections were not retained.

Recommendations – Grant Evaluation Processes

Ref.	Recommendation
1.1	The exceptions above should be considered for inclusion in the Council's Covid-19 lessons learned exercise and considered in the event that the Council is asked to manage and allocate future emergency Scottish Government grants.

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.