Governance, Risk and Best Value Committee

10.00am, Tuesday 10 August 2021

Internal Audit Annual Opinion for the year ended 31 March 2021

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

1. Recommendations

1.1 It is recommended that the Governance, Risk, and Best Value Committee (the Committee) notes the limited Internal Audit (IA) annual opinion provided for the year ended 31 March 2021.

Lesley Newdall

Head of Audit and Risk / Chief Internal Auditor

Legal and Assurance Division, Corporate Services Directorate

E-mail: lesley.newdall@edinburgh.gov.uk | Tel: 0131 469 3216

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Report

Internal Audit Annual Opinion for the year ended 31 March 2021

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.

2. Executive Summary

2.1 This report details IA's annual opinion for the City of Edinburgh Council (the Council) for the year ended 31 March 2021. The opinion is based on the outcomes of the audits completed as part of the Council's 2020/21 IA annual plan, and the status of open IA findings as at 31 March 2021.

2.2 The annual plan presented to the Committee in September 2020 recognised that plan delivery may need to be paused or amended in the event of another significant resilience incident, or to reflect the ongoing impacts of Covid-19. This flexibility has been applied as some services were unable to support completion of planned audits due to the ongoing impacts of Covid-19. As a result, only 80% of the 2020/21 IA annual plan has been completed to support the annual opinion. Additionally, a number of completed reviews were limited to assessing the design of controls, and did not consider their effectiveness. The impact of this reduced level of assurance is outlined in the main report.

2.3 Consequently, the 2020/21 opinion is a 'limited' opinion, recognising that the plan has not been substantially completed; that the outcomes include a number of reviews that were limited to assessing control design; and that it is not possible to pre-empt the potential outcomes of the remaining audits that comprise the remaining 20% of the plan. It is also important to note that completion of the remaining audits could potentially have resulted in a different annual opinion outcome. This approach is aligned with guidance from relevant professional bodies, and was also discussed and agreed at the June 2020 Committee.

2.4 IA's independent and professional opinion (based on limited completion of the 2020/21 annual plan) is that significant and / or numerous control weaknesses were identified in the design and / or effectiveness of the Council's control environment and / or governance and risk management frameworks. Consequently, only limited

assurance can be provided that risks are being identified and effectively managed, and that the Council's objectives should be achieved.

2.5 IA is therefore reporting a 'red' rated (significant enhancements required) limited opinion with our assessment towards the lower end of this category. This outcome is aligned with the limited 2019/20 IA opinion.

2.6 It is important to recognise that the Council has operated in an ongoing resilience environment implemented in response to the Covid-19 pandemic in March 2020 that has significantly changed the Council's risk profile, and has impacted both the design and effectiveness of the Council's established control environment and governance and risk management frameworks.

2.7 It is also important to note that this is the Council's fourth 'red' rated (significant improvement required) annual opinion, although some progress was evident with a move from the middle towards the lower end of this category between 2018/19 and 2019/20, and this position has remained consistent in the current year.

2.8 Whilst only 80% of the 2020/21 IA annual plan has been completed, the number of audits completed remains aligned with prior years, enabling comparison with prior year IA assurance outcomes.

2.9 The 2020/21 annual plan focused significantly on the design of new and amended services and processes that were implemented in response to Covid-19 (15 of the 32 completed reviews). The majority of these review outcomes were assessed as either 'effective' (green) or 'some improvement required' (amber), confirming that the Council implemented appropriately designed processes that were often urgently required in response to both Scottish Government and Public Health Scotland requirements and guidance that was regularly refreshed in response to the spread and impacts of the virus.

2.10 The 2020/21 annual opinion also includes the first 'inadequate' audit report outcome presented in the Council, which is based on the significance and volume of findings included in the relevant audit report.

2.11 No 'Critical' IA findings have been raised during the year, and the total number of findings raised has reduced in comparison with prior years, with a positive improvement evident in the proportion of High rated findings raised. However, this may be attributable to focus on design of controls in audits completed in 2020/21 with limited effectiveness testing

2.12 Whilst all 26 historic findings that were reopened in June 2018 have now been closed, an increase in the percentage of overdue IA findings as at 31 March 2020 is evident, together with a deterioration in their ageing profile. Consequently, further focus is required to ensure that the Council consistently addresses the risks associated with open IA findings by implementing agreed management actions within agreed timeframes.

2.13 As the annual validation review that confirms whether management actions implemented to address previously closed findings was not completed in 2019/20,

IA is unable to provide an opinion in this area. However, a number of recurring and new significant and thematic weaknesses have been identified in the Council's control environment.

2.14 This report is a key component of the overall annual assurance provided to the Council and there are a number of additional assurance sources that the Committee should consider when forming their own view on the design and effectiveness of the control environment, governance, and risk management arrangements across the Council.

2.15 This report has been prepared fully in line with Public Sector Internal Audit Standards (PSIAS) requirements, and IA has fully conformed with PSIAS requirements during the 2020/21 financial year.

3. Background

Internal Audit Objectives

3.1 The objective of IA is to provide high quality independent audit assurance over the control environment established to manage the Council's most significant risks, and their overall governance and risk management arrangements in accordance with PSIAS requirements.

3.2 The PSIAS provide a coherent and consistent IA framework for public sector organisations. Adoption of the PSIAS is mandatory for IA teams within UK public sector organisations, and PSIAS require annual reporting on conformance with their requirements.

3.3 It is the responsibility of the Council's Chief Internal Auditor to provide an independent and objective annual opinion on the adequacy and effectiveness of the Council's control environment and governance and risk management frameworks in line with PSIAS requirements. The opinion is provided to the Governance, Risk, and Best Value Committee and should be used to inform the Council's Annual Governance Statement.

3.4 Where control weaknesses are identified, IA findings are raised, and management agree actions and timescales by which they will address the gaps identified.

Management's Responsibility

3.5 It is the responsibility of management to address and rectify the weaknesses identified via timely implementation of these agreed management actions.

Overdue Internal Audit Findings

3.6 The IA definition of an overdue finding is any finding where all agreed management actions have not been implemented by the final date agreed by management and recorded in Internal Audit reports.

3.7 A total of 30 historic findings were reopened in June 2018 across both the Council (26) and the Edinburgh Integration Joint Board (4), where management actions agreed to address the risks associated with historic IA findings (dating back to 1 April 2016) had either not been implemented or had been implemented but not sustained.

2020/21 Internal Audit Annual Plan

3.8 The 2020/21 IA annual plan was approved by the Committee in September 2020. The plan recognised that only six months were available to support plan completion; that plan delivery may need to be paused or amended in the event of another significant resilience incident, or to reflect the ongoing impacts of Covid-19; and the importance of ensuring that the number of audits delivered remains aligned with the audits completed to support the 2019/20 limited IA annual opinion.

3.9 A total of 36 audits (excluding follow-up) were planned for completion across the Council. These included 5 of the 13 audits that were not completed in 2019/20 due to Covid-19, and the 11 Covid-19 audits that were approved by the Committee in June 2020.

3.10 During the year, a further 4 audits were added to the plan; 1 audit was removed and included in the 2021/22 annual plan; and two audits were combined, resulting in a total of 38 audits to be delivered across the Council. A full reconciliation of these changes is included at Appendix 5.

3.11 As the Council is the administering authority for the Lothian Pension Fund (LPF), our opinion also includes the outcomes of the two audit reviews performed for LPF and the status of their open audit findings as at 31 March 2021

3.12 Of the 40 audits to be delivered across the Council and LPF, 32 (80%) have been completed, with the remaining eight carried forward into the 2021/22 annual plan. These audits have been carried forward in response to the ongoing impacts of Covid-19 on the relevant services. Further detail on the audits carried forward into the 2021/22 annual plan are included at Appendix 6.

Other Assurance Providers

3.13 Internal Audit is not the only source of assurance provided to the Council as there are a number of additional assurance sources including: external audit, regulators and inspectorates, that the Committee should equally consider when forming their view on the design and effectiveness of the Council's control environment, governance and risk management arrangements.

The Three Lines Model

3.14 The Institute of Internal Auditors 'Three Lines Model' defines the first line in an organisation as those teams responsible for provision of products/services to clients, and managing risk; the second line as teams that provide expertise, support, monitoring and challenge on risk-related matters; and the third line as teams that provide independent and objective assurance and advice on all matters related to the achievement of objectives. This model can be translated across the

structure and operations of the Council with first line teams those responsible for ongoing service delivery and risk management; the second line those teams providing frameworks, policies and guidance (for example, the Information Governance Unit; Legal Services; Corporate Health and Safety; and Corporate Risk Management); and the third line, Internal Audit.

4. Main report

Impact of a Limited 2020/21 Internal Audit Annual Opinion

4.1 The 2020/21 IA annual opinion is a 'limited' opinion based on 80% completion (32 of a total of 40 planned audits) of the 2020/21 annual plan, which is directly attributable to the ongoing impacts of the Covid-19 pandemic. Additionally, the 11 Covid-19 audits that were approved by the Committee in June 2020 and the 3 Covid-19 grant reviews that were added to the plan were mainly limited to a review of control design and did not consistently consider control effectiveness.

4.2 The limited opinion recognises that it is not possible to pre-empt the potential outcomes of the remaining audits that comprise the 20% balance of the plan, and that completion of the remaining audits could potentially have resulted in a different annual opinion outcome.

4.3 This approach is aligned with Institute of Internal Audit (IIA) Covid-19 guidance; and the Chartered Institute of Public Finance and Accountancy (CIPFA) and the Internal Audit Standards Advisory Board (IASAB) joint guidance in relation to conformance with the PSIAS during the Covid-19 pandemic. The approach was also discussed and agreed at the June 2020 Committee meeting.

4.4 The overall impact of the 20% reduction in completion of the 2019/20 annual plan is reduced assurance on Health and Social Care; Customer and Digital Services; and Place Management, and reduced assurance in relation to health and safety (asbestos management) and the Council's fraud and serious organised crime risks.

4.5 Whilst only 80% of the 2019/20 IA annual plan has been completed, the total number of audits completed remains aligned with prior years (32 in 2020/21; 34 in 2019/20; and 37 in 2018/19), enabling comparison with prior year IA assurance outcomes as detailed below.

Basis of Internal Audit Annual Opinion

4.6 Our limited opinion is based on the outcomes of the 30 audits completed across the Council in the year to 31 March 2021, and the status of open IA findings as at 31 March 2021.

4.7 As the Council is the administering authority for the Lothian Pension Fund (LPF), our opinion also includes the outcomes of the two audit reviews performed for LPF and the status of their open audit findings as at 31 March 2021.

4.7.1 A separate IA opinion for the LPF is currently being prepared and will be presented at the Pensions Audit Sub-Committee in August 2021. This will be

an ‘amber’ rated (some improvement required) opinion, with our assessment towards the bottom of this category, reflecting an improvement from unchanged from the 2019/20 annual opinion where our assessment was towards the middle of this category.

4.7.2 This opinion reflects the outcomes of the two completed LPF audits completed audits with one assessed as ‘effective’ (green); and one as ‘some Improvement Required’ (amber); and the status of overdue LPF IA findings as at 31 March 2021.

4.8 No audits have been referred by the Edinburgh Integration Joint Board (EIJB) Audit and Risk Committee for inclusion in the 2019/20 IA annual opinion as the 3 reviews completed in the 2020/21 plan year had no direct impact on the services delivered by the Council as part of the Health and Social Care Partnership.

4.9 This opinion does not include audit reviews performed for arms-length external organisations that currently receive assurance from the Council’s IA team.

Internal Audit 2020/21 Annual Opinion

4.10 Based on limited (80%) completion of the 2020/21 annual plan, IA considers that significant improvements are required across the Council’s control environment, governance and risk management arrangements to ensure that the Council’s most significant risks are effectively identified, mitigated, and managed, and is raising a ‘red’ rated ‘significant improvement required’ opinion (see Appendix 1 category 3), with our assessment towards the lower end of this category.

4.11 This opinion remains aligned with the outcome reported for the 2020/21 financial year which was also a limited opinion based on 72% plan completion due to the initial impacts of the Covid-19 pandemic.

4.12 The majority of the outcomes of the Covid-19 reviews included in the 2020/21 annual plan were assessed as either ‘effective’ (green) or ‘some improvement required’ (amber), confirming that the Council urgently implemented appropriately designed processes in response to new legislative requirements and Scottish Government and Health Protection Scotland requirements and guidance. Only two Covid-19 review outcomes were assessed as significant improvement required’ (red).

4.13 Whilst one overall audit outcome has been assessed as ‘inadequate’ (black) based on the significance and volume of findings raised, no ‘critical’ IA findings have been raised. Additionally, the total number of findings raised in 2020/21 has decreased in comparison to the number of findings raised in prior years, with a positive improvement in the proportion of High rated findings raised. It is, however, important to note that this reduction may be attributable to IA focus on design of controls during 2020/21 with limited control effectiveness testing.

4.14 Whilst there has been deterioration in the percentage of overdue IA findings and their ageing profile as at 31 March 2021 in comparison to 2019/20, it is important to highlight that this is mainly due to management’s ongoing focus on the Council’s

Covid-19 operational resilience response. Whilst a four month extension timeframe was applied to all open IA findings to reflect the impact of the pandemic, it is likely that this was insufficient to reflect the ongoing impact on Council services and the reallocation of resources to focus on resilience activities.

4.15 A number of recurring new, significant, and thematic weaknesses have been identified in the Council's control environment, and further work is required to ensure that the Council consistently addresses the risks associated with open IA findings by implementing management actions to address these risks within agreed timeframes.

4.16 The findings raised in the 'inadequate' (black) IA report relate to the inconsistent application of the Council's established supplier management framework to support effective management of high risk contracts. These control gaps were initially highlighted by IA in a Council wide review completed in 2018/19, and the agreed management actions to address the risks identified have not yet been fully implemented. It is important to note that management contacted IA to request the addition of this review to the 2020/21 annual plan following an initial assessment of these supplier management risks, however these risks had been impacting the Council for some time and had not been previously identified and escalated.

4.17 Additionally, the concerns raised by the External Auditors, Azets, in their 2019/20 Risk Management audit have not yet been fully addressed as implementation of the refreshed operational risk management framework has been delayed to ensure appropriate ongoing focus on new and emerging Covid-19 risks and challenges.

4.18 It is acknowledged that the Council's Incident Management Team ensured that processes were established to identify; assess; record; and manage the new and emerging risks presented by the Covid-19 pandemic, however these processes have not been subject to review by IA.

4.19 Consequently, we believe that the Council's established control environment; governance; and risk management frameworks have not yet matured and adapted sufficiently to support effective management of the rapidly changing risk environment and the Council's most significant risks, putting achievement of the Council's objectives at risk.

4.20 It is IA's view that the weaknesses identified and highlighted in IA reports supporting the 2020/21 annual opinion are predominantly attributable to lack of capacity and skills within first line divisions and directorates to ensure that key controls; governance; and risk management processes are consistently and effectively applied to support effective ongoing management of service delivery and projects. This point was also raised in the 2018/19 and 2019/20 IA annual opinions, and it is essential that appropriate action is taken by management to ensure that this is addressed. The Council's Corporate Leadership Team has confirmed that they are in the process of implementing a revised first and second line governance and assurance model that should address these concerns.

Areas where improvement is required

4.21 The Council should endeavour to improve its control environment and governance and risk management frameworks to ensure that all significant risks are effectively recognised, managed, and mitigated, particularly across the areas highlighted below.

4.21.1 **Covid-19 response –** recognising that new processes and controls were implemented at a significant pace in response to new Covid-19 regulations and Scottish Government and Public Health Scotland requirements and guidance, and usually in addition to existing workloads, some areas were identified where the design and implementation of these controls could have been improved. These generally related to the identification of and management of risk, and governance and decision making processes. In some instances (for example supplier relief and physical distancing and employee protection) IA confirmed that the processes that had been designed were not consistently applied. These are highlighted in the following reports:

- Supplier Relief;
- Spaces for People;
- Shielding and Vulnerable Groups;
- Physical Distancing and Employee Protection;
- Allocation of Scottish Qualification Authority Grades;
- Workforce Management; and,
- Employee Testing.

4.21.2 **Governance**, **Decision Making and Scrutiny** – review of the management of the Council's external arm's length organisations (ALEOs) and the Governance, Risk, and Best Value (GRBV) Committee Effectiveness audits highlighted the need to ensure that appropriate second line frameworks are designed; implemented; and consistently applied by first line directorates to support effective management and scrutiny of the service delivery; financial and reputational risks associated with both the Council's subsidiary and other external companies that it engages with.

4.21.3 The GRBV Committee Effectiveness review also confirmed that whilst the Committee is fulfilling its core remit, there is opportunity to enhance the effectiveness of the scrutiny it performs and the impact it can achieve within the constraints of the overall design of the Council's scrutiny model.

4.21.4 **Supplier Contractor and Partnership Management** – the findings raised in the 'inadequate' (black) IA report relate to the inconsistent application of the Council's established supplier management framework to support effective management of high-risk contracts. These control gaps were initially highlighted by IA in a Council wide review completed in 2018/19, and the agreed management actions to address the risks identified have not yet been fully implemented.

4.21.6 It is important to note that these issues are not consistent across all contracts managed across the Council as the Public and Private Partnership (PPP) and Design, Build, Finance and Maintain (DBFM) Schools Contract Management review confirmed that these significant contracts were generally managed with some improvement required.

4.21.7 **Resilience** – review of the Council's Technology Resilience arrangements provided only limited assurance that the Council will be able to restore critical systems and services in line with expected timeframes in the event of a technology resilience incident, as recovery timeframes for systems supporting critical Council services have not been specified by services. Once specified, further discussion is required with Digital Services and CGI to confirm whether these are aligned with contractual recovery times agreed with CGI. Additionally, the Council's technology disaster recovery test plans require to be refreshed and tested.

4.21.8 Review of processes established across Council directorates to record Covid-19 resilience lessons learned also confirmed that some improvement is required as varying approaches are currently being applied by directorates in the absence of a corporate approach and supporting guidance. This report also highlights that a review of corporate lessons learned will be required to meet both Accounts Commission and COSLA expectations.

4.21.9 **Health and Safety** – review of the policies and processes established and applied in Education and Children's Services to prevent and manage behaviours of concern behaviour confirmed that the Council's violence at work policy requires to be refreshed and updated, and that Education and Children's Services policies and procedures should be refreshed consistently applied. It is also important to ensure that employees have sufficient capacity to complete training; that training completion is consistently monitored; that employees are aware of established complaints and escalation processes and available employee support arrangements; and that lessons learned are identified, recorded, and incorporated into risk assessments and pupil plans where appropriate.

4.21.10 It is important to highlight that management is aware that improvement is required in this area, and had already made some positive progress with their responses to the EIS and Unison employee unions 'Violence at Work' survey completed in 29 October 2018 and a subsequent elected member

motion on 11 December 2018. These were detailed in a report presented to the Education, Children and Families Committee in May 2019.

4.21.11 **Technology and Information** – review of network management arrangements to ensure the security of both the Council's corporate and learning and teaching networks confirmed that significant improvement is required. Whilst it is common for penetration testing to be performed annually to confirm whether known security vulnerabilities could potentially be exploited, good practice is to complete testing more frequently in conjunction with ongoing vulnerability scanning. Currently the Council relies on annual penetration testing performed on the Council's corporate network to support cyber essentials plus and public services network accreditation, and ongoing vulnerability scanning performed across both networks. No penetration testing is currently performed on the learning and teaching network to confirm whether known vulnerabilities identified from vulnerability scanning could be exploited. A number of additional areas were also identified where current network security controls could be improved.

4.21.12 **Service Delivery** - some weakness in service delivery controls were identified across all audits completed to support the 2020/21 IA annual plan, with details included in individual reports. It is also important to note that IA focus on new Covid-19 processes and controls means that there has been limited assurance provided on routine service delivery controls that could have been potentially impacted as a result of operating in the ongoing Covid-19 resilience environment.

Areas where positive assurance has been provided

4.22 The green or 'effective' reporting outcomes detailed below were achieved across the Council during the year. It is important to note that a number of these processes were essential to support the Council's Covid-19 response:

4.22.1 the design of Covid-19 grant processes implemented to provide support for businesses impacted during the pandemic;

4.22.2 arrangements for the procurement and allocation of protective personal equipment (PPE) to Council employees during the pandemic;

4.22.3 Scottish Government and COSLA Covid-19 returns processes;

4.22.4 the Employee Lifecycle Data and Compensation and Benefits processes (payroll) audit for the 2019/20 financial year confirmed that there were no significantly material or systemic errors in employee records and payroll transactions. It should be noted that a further review of salary overpayments confirmed that some improvement is required to ensure that Divisions/Directorates advise Human Resources of leaver details to ensure that they are removed from the payroll on time;

4.22.5 Chief Social Work Officer assurance and annual report; and,

4.22.6 Programme and Project Delivery - no new IA findings were raised during 2020/21 in relation to our ongoing agile audits of the Enterprise Resource Planning System and the Edinburgh Tram Extension projects, confirming that the control environments, governance, and risk management processes supporting these significant projects are operating effectively

IA Assurance outcomes

4.23 Of the 32 audits completed during the 2020/21 financial year, 12 (34%) were reported as 'effective' (green); 12 (41%) as 'some improvement required (amber); 7 (22%) as 'significant improvement required' (red); and one (3%) as 'inadequate' (black).

4.24 A total of 69 findings (16 High; 42 Medium; and 11 Low) were raised in the 32 audits completed.

4.25 Appendix 3 includes details of all 2020/21 audits completed (including those carried forward from 2019/20) for the Council (30 in total), and the outcomes of the 2 LPF reviews that will be provided to the Pensions Audit Sub-Committee for review and scrutiny.

Status of Internal Audit Findings as at 31 March 2021

4.26 There were 107 open IA findings across the Council as at 31 March 2021

4.27 All 26 historic Council findings that were reopened in June 2018 had been closed by 31 March 2021.

4.28 Of the 107 open IA findings:

4.28.1 a total of 43 (40%) findings were open, but not overdue;

4.28.2 a total of 64 (60%) were reported as overdue as they had missed all of their originally agreed implementation dates (17 High; 38 Medium; and 9 Low);

4.28.3 evidence in relation to 18 (42%) of the 43 overdue findings was being reviewed by IA to confirm that it was sufficient to support their closure; and

4.28.4 25 (58%) residual overdue findings still required to be addressed.

Comparison with Prior Year Outcomes

4.29 The 2020/21 IA annual opinion has slightly improved in comparison to the 2019/20 position, with IA's assessment now at the lower end of the red rated / significant improvement required category.

4.30 The rationale supporting this alignment considered the following IA assurance outcomes:

4.30.1 alignment between the total number of audits completed in the last three financial years (32 in 2020/21; 34 in 2019/20; and 37 in 2018/19) despite completion of only 80% of the 2020/21 annual plan;

4.30.2 the areas where improvement is required as detailed above;

4.30.3 closure of all 26 historic IA findings that were reopened in June 2018;

4.30.4 a decrease in the total number of IA findings raised, with 69 raised in 2020/21 in comparison to 83 and 82 in 2019/20 and 2018/19 respectively. It is important to note that this reduction may be attributable to focus on design of controls in audits completed in 2020/21 with limited effectiveness testing;

4.30.5 a decrease in the proportion of high rated findings raised, with 23% (16) raised in 2020/21 in comparison to 32% (27) and 37% (30) in 2019/20 and 2018/19 respectively. Again, it is important to note that this decrease may be attributable to focus on control design with limited control effectiveness testing;

4.30.6 an increase in the percentage of overdue IA findings, with 60% overdue as at 31 March 2020 in comparison to 49% in as at 31 March 2020; and

4.30.7 A deterioration in the ageing profile of overdue findings, with 42% more than one year overdue (18% in 2019/20), and 25% now more than six months overdue (14% in 2019/20) as the Council is not yet consistently addressing the risks associated with open IA findings by implementing management actions within agreed timeframes

Internal Audit Independence

4.31 PSIAS require that IA must be independent, and internal auditors' objective, in performing their work. To ensure conformance with these requirements, IA has established processes to ensure that both team and personal independence is consistently maintained and that any potential conflicts of interest are effectively managed.

4.32 IA does not consider that we have faced any significant threats to our independence during 2020/21, nor do we consider that we have faced any inappropriate scope or resource limitations (for example headcount restrictions) when completing our work.

4.33 Implementation of the governance process that requires approval of changes to the IA annual plan by both the Corporate Leadership Team and Governance, Risk and Best Value Committee in January 2018 also effectively supports ongoing IA independence.

Conformance with Public Sector Internal Audit Standards and IA Internal Quality Assurance

4.34 IA achieved full conformance with PSIAS requirements during the 2020/21 annual plan year following implementation of an internal quality assurance programme in 2019/20.

Internal Quality Assurance Outcomes

4.35 The 2020/21 internal quality assessment process focused on the consistency and quality of follow-up work performed by the IA team.

4.36 This involved review of follow-up work performed on a sample of nine management actions that had been closed following IA review during 2020/21. This sample reflects 5% of the full population of 177 findings closed, and comprised six high; two medium; and one low rated findings across all directorates (including LPF), with coverage across all IA team members and managers to assess whether file quality was compliant with the Council's IA methodology and PSIAS requirements.

4.37 The review was performed by three team members (with support and oversight from a Principal Audit Manager) who reviewed the follow-up work completed by other team members.

4.38 Files were assessed as either green (fully compliant); yellow (generally compliant); amber (partially compliant) and red (non-compliant) with the Council's IA methodology and PSIAS requirements.

4.39 The outcomes of the review confirmed that 22% of the files were fully compliant, and 78% generally compliant.

4.40 The themes identified from the reviews have been shared and discussed with the IA team, and will be reflected (where required) in individual team member development plans and ongoing monthly performance discussions.

4.41 The next IA external quality assessment is due for completion in 2021/22 in line with the five year review requirement specified in the PSIAS, and the Institute of Internal Auditors has been engaged to complete this review.

5. Next Steps

5.1 The remaining 20% of the 2020/21 has been carried forward into the 2021/22 annual plan. Work is currently underway on these audits. Progress with delivery of these reviews will be provided through the quarterly IA update report provided to the Committee and the outcomes will be reported to the Committee. Additionally, any reports that have either an overall red (significant improvement required) outcome or include any red (high) rated findings will be presented to the Committee for scrutiny in line with the process agreed with the Committee in July 2020.

5.2 IA will continue to monitor the open and overdues findings position, providing monthly updates to the Corporate Leadership Team, and quarterly updates to the Governance, Risk and Best Value Committee.

5.3 Whilst all IA reports with an overall significant improvements required (red) outcomes and those that include any high (red) rated findings have been formally presented to the Committee for review and scrutiny, elected members may not have had sufficient time to review all reports that do not meet these criteria, to determine whether they should be specifically requested for presentation at Committee. This is mainly attributable to the ongoing impacts of Covid-19 impacting finalisation of some reports.

5.4 Consequently, some reports may be presented to the Committee for review and scrutiny following their review of the 2020/21 IA annual opinion.

5.5 Details of the dates when IA reports were reviewed or made available for elected member consideration are included at Appendix 3.

6. Financial impact

6.1 Whilst there is no direct financial impact associated with the content of this report, it is important to note the indirect financial impacts (time and resources) associated with implementation of agreed management actions to address IA findings raised.

7. Stakeholder/Community Impact

7.1 As the 2020/21 annual opinion remains aligned with the 2019/20 assessment, this report highlights that the Council is currently exposed to a significant level of risk that puts achievement of its objectives at risk, and could potentially impact services delivered and support provided to citizens; stakeholders; community groups; and employees.

8. Background reading/external references

8.1 Internal Audit: Covid-19 Response – Paper 8.1

8.2 Internal Audit Annual Plan 2020-21- Paper 8.1

8.3 Public Sector Internal Audit Standards

8.4 Institute of Internal Auditors Three Lines Model

8.5 Internal Audit Opinion and Annual Report for the Year Ended 31 March 2020 – Paper 8.1

8.6 Internal Audit Opinion and Annual Report for the Year Ended 31 March 2019 – paper 11

8.7 Internal Audit Opinion and Annual Report for the Year Ended 31 March 2018 – item 7.11

8.8 Internal Audit Report - Historic Internal Audit Findings – item 7.3

9. Appendices

9.1	Appendix 1	Internal Audit Annual Opinion Definitions
9.2	Appendix 2	Limitations and Responsibilities of Internal Audit and Management Responsibilities
9.3	Appendix 3	Audits Completed Between 1 April 2020 and 31 March 2021
9.4	Appendix 4	IA Overdue Findings and Management Actions 31 March 2019 to 31 March 2021
9.5	Appendix 5	Summary of 2020/21 IA Annual Plan Changes
9.6	Appendix 6	Appendix 6 – Audits Carried Forward into the 2021/22 IA Annual Plan
9.7	Appendix 7	Covid-19 Supplier Relief Final Report
9.8	Appendix 8	Covid-19 Shielding and Vulnerable People Final Report
9.9	Appendix 9	GRBV Committee Effectiveness Final Report
9.10	Appendix 10	Salary Overpayments – Findings Only Final Report
9.11	Appendix 11	Technology Resilience Final Report
9.12	Appendix 12	Corporate and Learning and Teaching Network Management Final Report
9.13	Appendix 13	Arm's Length External Organisations Final Report
9.14	Appendix 14	Health and Safety Behaviours of Concern Final Report
9.15	Appendix 15	Covid-19 Spaces for People Final Report

Appendix 1 – Internal Audit Annual Opinion Definitions

The PSIAS require the provision of an annual Internal Audit opinion, but do not provide any methodology or guidance detailing how the opinion should be defined. We have adopted the approach set out below to form an opinion for Lothian Pension Fund.

We consider that there are 4 possible opinion types that could apply to the Council. These are detailed below:

1. 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.
2. 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.
3. 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.
4. 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.

Appendix 2 - Limitations and responsibilities of internal audit and management responsibilities

Limitations and responsibilities of internal audit

The opinion is based solely on the internal audit work performed for the financial year 1 April 2020 to 31 March 2021. Work completed was based on the terms of reference agreed with management for each review. However, where other matters have come to our attention, that are considered relevant, they have been taken into account when finalising our reports and the annual opinion.

Professional judgement is exercised in determining the appropriate opinion, and it should be noted that in giving an opinion, assurance provided can never be absolute for the reasons noted below:

1. Internal Audit endeavours to plan its work so that it has a reasonable expectation of detecting significant control weaknesses and, if detected, performs additional work directed towards identification of potential fraud or other irregularities. However, internal audit procedures alone, even when performed with due professional care, do not guarantee that fraud will be detected. Consequently, Internal Audit reviews should not be relied upon to detect and disclose all fraud, defalcations or other irregularities that may exist.
2. There may be additional weaknesses in the Council's control environment and governance and risk management frameworks that were not identified as they were not included in the Council's 2020/21 annual Internal Audit plan; were excluded from the scope of individual reviews; or were not brought to Internal Audit's attention. Consequently, management and the Committee should be aware that the opinion may have differed if these areas had been included or brought to Internal Audit's attention.
3. Control environments, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and the impact of unplanned events.

Future periods

The Internal Audit opinion is based on an assessment of the controls that operated across the Council during the year ended 31 March 2021. This historic evaluation of effectiveness may not be relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Management responsibilities

It is management's responsibility to develop and operate effective control environments and governance and risk management frameworks that are designed to prevent and detect current and future irregularities and fraud. Internal audit work should not be regarded as a substitute for these responsibilities.

Appendix 3 - Audits completed between 1 April 2020 and 31 March 2021

			No. of findings raised				Report Available for Scrutiny
	Review Title	Report Outcome	High	Medium	Low	Totals	
Ref	**Council Wide**						
1.	Covid-19 Newly Self-Employed Grant Application Process (Design Review)	**Effective**	-	-	1	1	May 2021
2.	Covid-19 Procurement and Allocation of Personal Protective Equipment	**Effective**	-	-	1	1	May 2021
3.	Covid-19 Workforce Management	**Some Improvement Required**	-	1	-	1	May 2021
4.	Covid-19 Employee Testing	**Some Improvement Required**	-	1	1	2	June 2021
5.	Covid-19 Support for Business Grants – pre-implementation review of the design of the new process.	**Effective**	No significant control design weaknesses were identified that would have impacted implementation of the new process. IA advice on areas where controls could potentially be improved was provided to management for consideration, and no audit reports were prepared				
6.	Covid-19 – Taxi and Private Hire Driver Support Fund - pre-implementation review of the design of the new process	**Effective**					
7.	Covid-19 – Discretionary Business Grants - pre-implementation review of the design of the new process	**Effective**					
8.	Covid-19 Supplier Relief	**Significant Improvement Required**	1	1	-	2	May 2021
9.	Covid-19 Shielding and Vulnerable People	**Some Improvement Required**	1	2	-	3	May 2021
10.	Covid-19 Lessons Learned	**Some Improvement Required**	-	1	-	1	July 2020
11.	Covid-19 Physical Distancing and Employee Protection	**Some Improvement Required**	-	3	-	3	July 2020
12.	Governance, Risk, and Best Value Committee Effectiveness	**Significant Improvement Required**	-	9	2	11	August 2021
	Totals		**2**	**18**	**5**	**25**	

	Review Title	Report Outcome	No. of findings raised				Report Available for Scrutiny
			High	Medium	Low	Totals	
	Corporate Services						
13.	Employee Lifecycle Data and Compensation and Benefits Processes for the 2019/20 Financial Year	**Effective**	-	1	-	1	May 2021
14.	Digital Services Change Implementation	**Some Improvement Required**	-	2	-	2	May 2021
15.	Public and Private Partnership (PPP) and Design, Build, Finance and Maintain (DBFM) Schools Contract Management	**Some Improvement Required**	-	1	-	1	May 2021
16.	Salary Overpayments – Findings Only report	**Some Improvement Required**	1	-	-	1	June 2021
17.	Technology Resilience	**Significant Improvement Required**	1	3	-	4	August 2021
18.	Corporate and Learning and Teaching Network Management	**Significant Improvement Required**	2	2	-	4	August 2021
19.	Direct Access and Mobile Device Management	**Some Improvement Required**	-	2	2	4	August 2021
20.	Covid-19 Scottish Government/COSLA Returns	**Effective**	-	1	-	1	June 2021
21.	Arm's Length External Organisations (ALEOs)	**Significant Improvement Required**	2	-	-	2	August 2021
	Totals		**6**	**12**	**2**	**20**	
	Education and Children's Services						
22.	Covid-19 Allocation of estimated SQA grades	**Some Improvement Required**	-	1	-	1	May 2021
23.	Health and Safety – Behaviours of Concern	**Significant Improvement Required**	2	1	-	3	August 2021
24.	Chief Social Work Officer Assurance and Annual Report	**Effective**	-	-	2	2	June 2021
	Totals		**2**	**2**	**2**	**6**	
	Health and Social Care Partnership						
25.	Covid-19 - HSCP Command Centre	**Some Improvement Required**	-	2	-	2	May 2021
	Totals		**-**	**2**	**-**	**2**	

	Review Title	Report Outcome	No. of findings raised				Report Available for Scrutiny
			High	Medium	Low	Totals	
	Place						
26.	Registration and Bereavement Services	**Some Improvement Required**	-	2	1	3	May 2021
27.	Covid-19 Spaces for People	**Significant Improvement Required**	1	2	-	3	July 2021
28.	Edinburgh Tram Network Infra-company Supplier Management Arrangements	**Inadequate**	4	1	-	5	August 2021 'B' Agenda item
	Totals		**5**	**5**	**1**	**11**	
	Projects						
29.	Enterprise Resource Planning System – ongoing agile audit	**Effective**	-	-	-	-	Ongoing
30.	Tram to Newhaven – ongoing agile audit	**Effective**	-	-	-	-	Ongoing
	Totals		**-**	**-**	**-**	**-**	
	Lothian Pension Fund						
31.	Bulk Transfers	**Effective**	-	1	1	2	August 2021
32.	Cessations	**Some Improvement Required**	1	2	-	3	August 2021
	Totals		**1**	**3**	**1**	**5**	
	Total Findings Raised 2020/21 – 32 Audits		**16**	**42**	**11**	**69**	
	2019/20 Total – 34 Audits		**27**	**38**	**18**	**83**	
	2018/19 Total – 37 Audits		**30**	**32**	**20**	**82**	

Appendix 4 – IA Overdue Findings and Management Actions from 31 March 2019 to 31 March 2021

	Key Performance Indicator (KPI)	31/03/2019		31/03/2020		31/03/2021		Trend
	IA Findings							
1	Open findings	83	100%	85	100%	107	100%	Not Applicable
2	Not yet due	32	39%	43	51%	43	40%	Not Applicable
3	Overdue findings	51	61%	42	49%	64	60%	
4	Overdue - IA reviewing	20	39%	7	16%	18	28%	
5	High Overdue	13	28%	15	36%	17	27%	
6	Medium Overdue	33	57%	23	54%	38	59%	
7	Low Overdue	5	15%	4	10%	9	14%	
8	<90 days overdue	4	8%	13	31%	11	17%	
9	90-180 days overdue	8	16%	5	12%	10	16%	
10	180-365 days overdue	14	27%	6	14%	16	25%	
11	>365 days overdue	25	49%	18	43%	27	42%	
	Management Actions							
12	Open actions	209	100%	221	100%	296	100%	Not Applicable
13	Not yet due	98	47%	117	53%	120	41%	Not Applicable
14	Overdue actions	111	53%	104	47%	176	59%	
15	Overdue - IA reviewing	26	23%	16	15%	61	35%	
16	Latest date missed	45	41%	35	34%	95	54%	
17	Date revised > once	54	49%	33	32%	71	40%	

Trend Analysis - Key

- Adverse trend - action required
- Stable with limited change
- Positive trend with progress evident

No trend analysis is performed on open findings and findings not yet due as these numbers will naturally increase when new IA reports are finalised

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Appendix 5 – Summary of 2020/21 IA Annual Plan Changes

2020/21 IA annual plan changes	Council	ALEOs	Total
Audits included in original plan approved in September 2020	36	9	45
Audits added to the plan • Edinburgh Tram Network Supplier Arrangements (approved Dec 20) • Covid-19 Taxi and Private Hire Support Fund design review (February 21) • Discretionary Grants design review (February 21) • Salary Overpayments – findings only review (February 21)	4	-	4
Audits combined / removed from the plan • Corporate and Learning and Teaching Technology Network Management reviews (combined) • Development and Implementation of the Council's Carbon Neutral / Climate Change Strategy – removed and included in 2021/22 plan (approved March 2020)	(2)	-	(2)
Total audits remaining in 2020/21 IA annual plan	38	9	47

Appendix 6 – Audits Carried Forward into the 2021/22 IA Annual Plan

Audits carried forward into the 2021/22 IA Annual Plan		
1.	Council Tax and Business Rates	Audit in progress. Aiming to complete by end August 21
2.	Development of the Council's Digital and Smart Cities Strategy	Audit in progress. Aiming to complete by end August 21
3.	Health and Safety - Implementation of asbestos recommendations (PwC)	Audit in progress. Aiming to complete by end August 21
4.	Parking and Traffic Regulations	Audit in progress. Aiming to complete by end August 21
5.	Management of waiting lists and assessments (HSC)	At planning stage. Aiming to complete by end September 21
6.	Fraud and Serious Organised Crime (including Physical Security controls)	At planning stage. Aiming to complete by end September 21
7.	Active Travel – Project Management and Delivery	At planning stage. Aiming to complete by end September 21
8.	Adaptation and Renewal Programme Governance	Not yet started

The City of Edinburgh Council

Internal Audit

COVID19 006 Supplier Relief
28th May 2020

Overall Report Rating:

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.**

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Covid-19

Supplier Relief

Findings Raised: - | 1 | 1 | -

Background

On 26 March 2020, the Scottish Government published their Scottish Procurement Policy guidance Note (SPPN) 5/2020 for public bodies that provided guidance notes for Local Authorities to support supplier service continuity during Covid-19. The Convention of Scottish Local Authorities (COSLA) also issued a set of Principles to Council's that are aligned with the SPPN.

The key points included in the SPPN guidance note are:

1. suppliers must set out proposals to vary an existing contract or request some form of relief;
2. suppliers will not be entitled to combine a relief under the contract with any other COVID-19 related relief which results in receipt of more than one benefit / relief for the same underlying cash-flow issue;
3. suppliers must have evidence that any monies paid have been used as intended; and
4. suppliers must promptly pay their staff and supply chain; and
5. monies paid can be recovered by public bodies in certain circumstances, e.g. supplier breach of contract.

The Council's Supplier Relief process was designed to provide urgent and immediate support to critical suppliers and was aligned with both SPPN and COSLA guidance.

The Council's Incident Management Team (CIMT) approved implementation of the process on 2 April 2020, and confirmed that:

1. early learning; childcare; and social care suppliers and specialist transport service providers supporting front line services in sectors/locations where there is a lack of alternative suppliers, should be engaged and prioritised;
2. there should be focus on payments to small and medium enterprise suppliers;
3. all payments should be approved by relevant Executive Directors; the Head of Finance; and the Chief Procurement Officer, and would be met from existing service budgets.

Supplementary guidance (SPPN 8/2020) was issued on 30 June which provides guidance on Covid-19 transitional arrangements and restarting contracts; endorses unlimited extension of established supplier relief arrangements beyond 30 June; and encourages implementation of future longer-term commercially sustainable supplier arrangements. The Council's response to SPPN 8/2020 was approved by CIMT on 26 June 2020.

Scope and approach

Scope

Review of the design of key supplier relief process controls to confirm that the process was designed and implemented in line with applicable guidance, and mitigated the following key risks::

- Financial risk – risk that demand for support exceeds funding available to support the supplier relief process or has an adverse impact on the Council's cash flow;
- Fraud risk – receipt of fraudulent (overstated) or inaccurate claims (e.g. where suppliers already receive other COVID-19 related relief);
- Resourcing risk – adequacy of appropriately skilled and experienced resources to process the volume of applications received;
- Decision making – risk that incorrect decisions will be made on applications received; and
- Processing risk – risk that payments are not processed accurately.

Approach

- Discussion with management to understand their risk appetite in relation to the process. As no risk appetite was specified, our approach assumed that full compliance with the established process was required.
- A walkthrough of the end to end process to identify and understand the design of key process controls and validate the outcomes for a sample of supplier relief applications;
- Review of a sample of two completed applications with a combined valued of £270K to assess whether the key controls were adequately designed and implemented to mitigate the key risks and were aligned with management's risk appetite.
- Identification of areas where the design and implementation of the controls require improvement

Opinion

Our review confirmed that the supplier relief process was effectively designed, despite tight implementation timeframes, with appropriate application validation controls established to support effective assessment of claims received prior to payment. Additionally, these controls were aligned with both SPPN 5/2020 and COSLA guidance,

However, the process approved by the Council's Incident Management Team (CIMT) was not consistently applied.

It is acknowledged that this may be attributable to the complexity of the process and the urgency to provide immediate support for suppliers during the initial lockdown phase of the Covid-19 pandemic. Additionally, the processes applied were generally aligned with both SPPN and COSLA guidance, with the exception of confirming that suppliers were not in receipt of any other government grants or funding as (in some instances) attestation from suppliers was accepted to support supplier relief payments.

Management has provided rationale for and confirmed that they are comfortable with the potential risks associated with these variances from the approved process, however these variations have not been recorded and approved.

Consequently, one High and one Medium rated findings have been raised .

The high rated finding highlights the need for a proportionate retrospective review to identify any excessive and / or inappropriate payments; suppliers who have not used funds in line with agreed terms and conditions; and explore potential recourse options (where appropriate).

The Medium rated finding focuses on the need to complete the Supplier Relief Register that forms the basis of Scottish Government reporting on the volume and value of payments made, and ensure that appropriate arrangements are made for central storage and retention of all supplier relief documents.

Areas of good practice

- Comprehensive and timely response to SPPN and COSLA guidance;
- Proactive consultation with stakeholders and CIMT on process design; and
- Comprehensive guidelines prepared and issued

Detailed Findings

1. Supplier Relief Claims – Application Processing Controls

Observations

The Council's supplier relief process requires divisions to review applications and confirm whether conditions are achieved before submitting requests for approval and payment to directors. Terms or conditions can be waived in extenuating circumstances following completion of appropriate due diligence and provision of rationale to support management review and decision making.

Review of two supplier relief claims, assessed by divisions and validated by Commercial Procurement Services (CPS) and Finance prior to approval by the Executive Director of Communities and Families confirmed that the established process was not consistently applied. Specifically:

- **Variable costs** - supplier claims were not consistently adjusted to remove variable costs. Management advised that this was due to the complexity involved and urgency to make payments; and that payments to transport providers were adjusted to reflect reduced fuel costs for adjusted routes.
- **Other Covid-19 relief** - claims were accepted that disclosed receipt of Job Retention Scheme support. Management advised that these suppliers operated both public and private sector transport contracts, and that support was provided for employees working on private sector contracts. Whilst management also confirmed that the Executive Director was verbally advised prior to approval of the payment, the rationale supporting the decision to make these supplier relief payments has not been documented.
- **Contractual status** - payments were made to suppliers operating under a procurement framework who did not have an established fixed contract with the Council. Management has advised that these suppliers received payment as they provided regular transport services, however, this decision was not documented.
- **Ongoing supplier monitoring -** was not performed to confirm that suppliers in receipt of payments continued to meet the Council's supplier relief requirements specified in the SPPN guidance and contract change notices provided to suppliers.

Recommendations

1. In relation to supplier relief payments made, CPS and Finance should consider:
   - jointly perform a risk-based retrospective review of completed applications to determine whether any excessive supplier relief payments have been made; and
   - where excessive payments or inappropriate use of funds is identified from retrospective reviews, consult with divisions Legal Services to understand the available options to pursue (where relevant) partial or full recovery of funds.
2. For the ongoing supplier relief process:
   - CPS should design an application checklist, aligned with SPPN and COSLA guidance and the established Council process, for service areas to complete when processing a new application.
   - CPS should communicate the requirement for completion and provision of the checklist together with supporting documentation and rationale; and
   - CPS and Finance should review checklist completion for a risk based sample of complex; high risk; and high value applications prior to payment and document their reviews.
3. Service areas and directorates should complete the processing checklist to confirm process compliance and consider to perform risk based review to confirm if suppliers have used their relief funds appropriately and in line with the agreed terms detailed in CCN.

Risks

The potential risks associated with our findings are:

- payments are made to non critical suppliers who do not meet either the Council's terms and conditions or COSLA and / or SPPN 5/2020 guidance.
- excessive payments are made to cover variable costs and profit margins.
- reputational damage associated with inappropriate allocation of funds to suppliers and their inappropriate use by suppliers.

Management Comments

Please refer slide 4.

Management Comments

1. Supplier Relief Claims – Application Processing Controls

The Internal Audit observations principally relate to relief to partner providers of critical external transport services. The Council's arrangements in this key area reflect COSLA's policy commitment to support partner providers with particular emphasis on delivery of public services necessary to tackle Covid-19. The Council's Supplier Relief scheme reflects COSLA's policy position with CIMT directing that special consideration be given to suppliers supporting the delivery of services to children and vulnerable citizens and agreeing that the Council would pro-actively engage with relevant Early Learning and Childcare suppliers, social care suppliers, suppliers of supported bus service and suppliers of other specialist transport services in areas where it was considered that action was needed in order to protect the availability of vital front-line services.

In line with COSLA policy and CIMT direction, Council officers engaged with critical transport providers to assess support required. Requests for support were required to reflect, as a minimum, savings in variable costs such as fuel and maintenance. While the Council engaged with 38 transport providers to assess support required on an individual basis, it should be noted that local authorities adopted a range of approaches with some local authorities adopting a simpler approach by agreeing to pay a set percentage (typically 75% - 100%) of regular payments to all transport providers.

The audit findings relate to supplier relief payments to transport providers in the initial phase (April 2020 to June 2020) of the Covid-19 pandemic. The audit observations are attributable to the complexity of the process; the emerging and changing position on national support schemes; the diverse organisational circumstances of the partner organisations requesting relief; and the urgency to provide immediate support to ensure service continuity, protect infrastructure, supply chains and jobs.

In relation to the risks identified by Internal Audit, it should be noted that: all payments were made to critical suppliers of regular transport services; payments to transport providers averaged 84% of regular payments (with this being broadly in line with arrangements implemented by other local authorities); relief provided was in accordance with the COSLA policy position and the CIMT decision to proactively engage with transport providers; all relief payments were subject to Contract Change Notices which set out the terms of the payments and provided for recovery of any overpayment; relevant service areas are responsible for ensuring appropriate operational oversight in relation to the application of the relief as part of their ongoing contract management responsibilities; relief provided has supported the policy objective of protecting critical front-line services with partner transport providers continuing to support education recovery.

Given the circumstances outlined above, management in CPS and Finance do not plan to undertake retrospective reviews of relief applications or the other recommended actions. As noted above, in hindsight a simpler "set percentage" relief arrangement may have been appropriate for partner providers of critical services and this will be considered further in the design of any future schemes.

Ongoing supplier relief claims are minimal and no process changes will be taken forward at this time. CPS will, however, write to Heads of Services to remind them of the existing process, direct them to the information which is available on the Orb and ask this be cascaded.

Detailed findings

2. Supplier Relief Claims - Records Management

Observations

Requirement for completion of a data privacy impact assessment (DPIA) was considered by management as part of the process design, but was not considered necessary as the information collected, processed, and stored was either publicly available, or would have been gathered during established supplier management processes.

Review of record-keeping and information governance arrangements established to support the supplier relief process confirmed that:

- the Supplier Relief Register (SRR) which is a key document for monitoring expenditure and is a source of data for Scottish Government statistical returns has not been regularly updated. In some cases, the SRR includes only the first application and payments made suppliers, and does not include subsequent applications and payments.
- no written records are kept to evidence completion of each stage with the application processing in line with procedural guidance, and
- the majority of supplier relief documentation is stored in individual email accounts.

During our process walkthrough, a service manager also expressed concerns regarding a potential duplication of efforts in reporting the status of supplier relief payments by each service area/directorate to their respective Executive Committees and CIMT, as this involves significant management effort and limits time available to focus on process oversight and assurance.

Recommendations

The following recommendations should be implemented to retrospectively address gaps in record keeping and governance arrangements supporting the supplier relief process:

1. CPS should update the Supplier Relief Register with details of all the approved; rejected; and paid claims.
2. Service areas/directorates, CPS and Finance teams should store all relevant documents and information supporting received and processed claims in a central location such as departmental shared drives. This should include (but not be limited to) signed application forms and supporting documentation; signed Contract Change Notices; pre-approval supplier criticality and financial risk assessments; and relevant email conversations.
3. CPS should consider potential efficiency of centralising the supplier relief payments reporting to CIMT and other relevant governance committees.

Risks

The potential risks associated with our findings are:

- the Council cannot confirm the total volume of supplier relief claims received; processed; and the total value of payments made.
- incomplete and / or inaccurate Scottish Government returns.
- inability to source documentation to support retrospective review and potential recovery of funds where excess payments have been made, or funds have not been used appropriately by suppliers, and
- duplication of efforts and inefficient use of management time.

Management Comments

As noted, CIMT approved the supplier relief process, which was then cascaded to service areas, with individual Directorates being responsible for ensuring the agreed process was followed and individual applications for relief subject to the approval of the relevant Executive Director and/or CIMT.

The Supplier Relief Register has been updated with details of all known claims, albeit confirmation is awaited from three service areas in respect of aspects of individual claims. CPS will, as part of the reminder referred to in the previous action, ask that services again review the Supplier Relief Register to confirm completeness of the register.

As regards the recommendation that all relevant documents and information be stored in a central location, this is a matter for relevant service areas to consider and undertake as part of their ongoing contract management arrangements. CPS do not consider that there is a need to store relevant documents and information in a central location. Likewise, CPS do not consider there is a need to formally review the supplier relief process for further efficiencies. However, in the usual way, this will be kept under review, as with all operational procedures, to ensure it is appropriate.

As noted above, supplier relief payments reporting is centralised within directorates with proposals to be signed off by Executive Directors in the first instance with Directorate recommendations then being considered through CIMT where appropriate. CPS will remind all services areas that final approval of any supplier relief payments should continue to be approved through CIMT where appropriate.

Appendix 1

Basis of our classifications

Finding Rating	Assessment Rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation of the Council which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation of the Council.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the Council.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the Council. •

The City of Edinburgh Council
Internal Audit

COVID-19 Shielding and Vulnerable People

Draft Report

28th May 2021

Overall report rating:

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.

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Covid-19 Shielding and Vulnerable People

Findings Raised: - 2 1 -

Background

Shielding

In response to Covid-19, the Scottish Government (SG) implemented a shielding approach to ensure that citizens at highest risk from COVID-19 were protected. This involved identifying those citizens most at risk and asking them to stay at home because the infection rate within the community was so high.

Scottish Local Authorities were asked by the SG to implement processes to ensure that those at highest risk received support through delivery of food supplies; essential medication; and basic supplies and services.

The SG worked with the NHS to identify those citizens whose underlying health conditions meant they were at highest clinical risk for COVID-19 and would be advised by the government to self-isolate. All citizens identified were contacted by SG letter.

Shielding was paused in Scotland from 1st August, and details of the SG shielding route map for those at highest risk are available at Scottish Government Shielding Route Map

Vulnerable People

The Council also recognised (as supported by the SG) that there would be a population of non shielding vulnerable citizens who may also require support. Arrangements to support these vulnerable citizens were established with Volunteer Edinburgh and the Edinburgh Voluntary Organisations Council (EVOC), with Memorandums of Understanding established to confirm how these arrangements would operate.

The Council published its guidance on support for both shielding and vulnerable people and relevant contact details on the Council's website information-for-vulnerable-and-high-risk-people.

Scope and approach

Scope

This review assessed the design adequacy of key controls established to support the Council's shielding and vulnerable people (SVG) Programme, and confirm whether these were designed in line with both SG and Health Protection Scotland guidance and requirements.

The review also considered whether the following key risks were appropriately mitigated in line with management's risk appetite:

1. **Financial risk** - Risk that financial implications associated with provision of shielding support are not clearly understood; and the Council cannot recover all costs incurred.
2. **Reputational risk** - SG requirements to protect shielded citizens are not achieved, and vulnerable citizens are not identified and supported.
3. **Resourcing / Service delivery risk**
   - Eligibility of Support Requests
   - Data Capture, Management and Use
   - Workforce capacity and skills
   - Public safety risk (including Covid-19 infection)
   - Supply Chain
   - Information Governance
   - Programme Governance
   - Lessons Learned

Approach

The following audit approach was applied:

1. Discussion with management to understand their SVG risk appetite.
2. Process walkthroughs to identify and understand the design of key controls.
3. Assessment to confirm whether key controls were adequately designed to mitigate the key risks, and are aligned with risk appetite.
4. Identify areas where control design should be improved.
5. Make proportionate recommendations for management to consider as part of SVG lessons learned.

Opinion

Completion Date

Audit work was completed by 21 January 2021, and our opinion and findings are based on the Programme information available as at that date

Opinion

Whilst some significant and moderate control weaknesses were identified in the design of the SVG Programme control environment and governance and risk management frameworks, they provide reasonable assurance that risks were managed, and that the Council's objectives to support shielding and vulnerable citizens from the start of the March lockdown (circa 15 March) through to 1 August (for shielding citizens) and 21st September (for Vulnerable Groups) were achieved.

Implementation of the separate SVG Programmes (that were subsequently combined) was an urgent resilience response to new and continually evolving SG shielding requirements and the Council's focus on protecting vulnerable citizens. The Programme was also implemented when the Council was managing Covid-19 workforce impacts and other significant service delivery and funding risks that could have adversely impacted the effectiveness of the Council's SVG response.

The Programme should be commended on the timeliness of its response and the willingness of all involved to protect and support citizens from Programme board members and senior management to catering teams preparing food boxes. Other teams involved in establishing and coordinating this urgent response included contact centre teams; Digital Services; delivery drivers; ATEC 24 Sheltered Housing and Community Alarm Services; and the voluntary organisations who provided additional support for vulnerable citizens.

The one High and two Medium rated findings raised highlight areas where improvement is required in relation to Programme governance; risk management; records management; the design and implementation of the shielding contact process; and engagement with and oversight of third party voluntary organisations.

Whilst the Shielding and Vulnerable Groups programme is now closed, with Vulnerable Groups now included within the Immediate Support group, it is important that Programme lessons learned (including the points highlighted in this report) are recorded and retained as part of the Council's overarching resilience plans in the event that a similar programme is initiated in response to a future resilience event.

Areas of good practice

- The pace of implementation given constantly evolving SG requirements.
- The move from manual to automated record keeping processes to support the Programme.
- ATEC24 was proactive in contacting vulnerable citizen's and completed over 34,000 telephone wellbeing calls to citizens between 24th March and 30th September 2020.
- Management advised that the shielding list is being maintained with support from the NHS in the event that shielding is reinstated.

Management Response

An overarching management response is included at page 3.

Overarching Management Response

Shielding and Vulnerable Groups

The City of Edinburgh Council, like other Scottish Local Authorities, was directed by the Scottish Government to rapidly implement and support a range of new and additional services to support those people identified as clinically shielded or vulnerable in response to the Covid-19 pandemic. The Scottish Government national guidance and approach was developed at pace and changed regularly, at times daily, throughout the period of the pandemic and this meant that the Council was often required to amend, adjust or otherwise change what it was doing, at times with no or very limited notice. The Council's primary responsibility throughout this period was to ensure that the services for shielded and vulnerable individuals were implemented rapidly and that these individuals were supported effectively. The overriding concern throughout this programme of work remained the safety and support needs of these individuals. Applying a complete and full programme management approach and all of the necessary controls and checks had to be balanced pragmatically by Council Officers against delivering the priority needs and positive outcomes for the individuals being supported. Whilst there will be opportunities for improvement and learning to be gained, any management actions identified are set within the context that the Council delivered new and additional essential services, during a global pandemic, which achieved the outcome of supporting shielded and vulnerable people and families across the City.

Detailed findings

1. Programme Governance and Risk Management

Observations

Whilst it is recognised that the Shielding and Vulnerable Groups Programme was initially established as two separate projects that subsequently combined, and that both were initiated urgently in response to Scottish Government (SG) shielding requirements and the Council's concerns regarding vulnerable groups, review of Programme governance arrangements established that:

Shielding and Vulnerable Groups

1. **Risk Appetite** - an overarching risk appetite for the Council's shielding and vulnerable citizens response was not defined, although management has confirmed that the key Programme objective was to ensure that all published Scottish Government requirements and guidance to support shielding citizens were met and applied.
2. **CIMT decisions and actions** - no process was established to ensure that Council Incident Management Team (CIMT) decisions and actions required in relation to shielding and vulnerable group programme activities were fed back into the programme and completed.

Vulnerable Groups

3. **Records Management** - four sets of board papers for the initial Vulnerable Groups (VG) board (between April and May 2020) could not be located. Consequently, we were unable to confirm that the VG pathway document (a key document that details the Council's response to vulnerable groups during the March 2020 lockdown) was reviewed and approved by the board. Management has advised that the pathway document was reviewed and approved by the board on 28 April 2020.
4. **Risk Management** - risks in relation to vulnerable citizens who were not shielding (for example, the potential risk that vulnerable citizens as defined by the SG known to the Council and / or their families were contacted by the Council) and the processes implemented to address them, were not identified; assessed; and recorded.
5. **Financial Virements –** discussions with Finance highlighted that vulnerable groups food costs incurred (£1.65M) have still to be transferred from Corporate budget to the Resources budget.

Shielding

6. **Application of guidance** - no clear link was evident to demonstrate how SG shielding guidance was translated into programme decisions and actions.
7. **Change Prioritisation** - criteria was not evident to support clear prioritisation for implementation SG changes to shielding requirements discussed during programme boards.

Recommendations

In the event that the shielding and vulnerable groups programme is reinstated either in response to Scottish Government requirements; the Council's response to Covid-19; or if a similar programme is implemented in response to a future resilience incident, it is recommended that the Programme:

1. Identifies and considers all potential risks associated with the requirements or proposed response, and establishes a risk appetite that clearly defines the level of risk it is prepared to accept based on urgency; workforce capacity; and availability of other resources (for example funding) available to support implementation and delivery.
2. Establishes a process to ensure that new and emerging risks across all aspects of the Programme are identified; assessed; recorded; and effectively managed.
3. Establishes an agreed records management and retention process to ensure that key programme governance documents can be easily retrieved.
4. Establishes a process that clearly demonstrates how relevant regulations, legislation, and guidance is considered and translated into programme decisions and actions.
5. Vulnerable Groups financial virements should be completed prior to the financial year end (31 March 2021).
6. Establishes criteria to assess and prioritise implementation of actions in response to changes in regulations, legislation, guidance, and actions required to support relevant CIMT decisions. Action required to implement these changes and decisions could potentially be prioritised and implemented in line with the Programme's risk appetite (refer finding 1).

Risks

The potential risks associated with our findings are:

- **Programme Governance** – risk that the Programme may have taken an unacceptable level of risk given urgency required when implementing and delivering the shielding and vulnerable groups Covid-19 response.
- **Programme Governance** – risk that new and emerging risks were not identified; assessed; recorded and effectively managed during the lifespan of the Shielding and Vulnerable Groups Programme.
- **Information Governance** – records are not available to support the rationale for key programme board decisions taken in a resilience situation
- **Programme Governance** – vulnerable groups costs are not allocated to the correct centre in the general ledger
- **Programme Governance** – the Programme is unable to clearly demonstrate that all applicable regulations; legislation; guidance; and CIMT decisions and actions (including subsequent changes) have been translated, prioritised, and incorporated into programme decisions and actions.

Management Comments

1. Accept that the risk appetite for the Programme was implicit and not explicit. A risk register was developed for Shielding, but not for Vulnerable Groups. Risk was discussed for Vulnerable Groups, but risks and decisions were not recorded.
2. This was achieved informally through both Executive Directors attending CIMT and feeding back to the Programme Board. Agree that there was no clear linkage between the CIMT action tracker and the Boards. Some Programme actions were agreed at the express instruction / request of CIMT and were not included in scope.
3. Agree that 23 and 28 April folders with board minutes cannot be located. E mails have now been located with Board papers and minutes from 28 April that include details of the actions.
4. Agree that this risk was not recorded, although there were implicit risk discussions with Customer teams on use of the Verint system.
5. Finance has now confirmed that these transfers have been processed.
6. A process was applied where weekly guidance was reviewed and discussed at daily calls, and actions would have been discussed at the Board. Agree that verbal discussions and decisions were not always recorded.
7. This wasn't an issue as the Programme simply implemented the SG changes as they were announced. There was limited time for initiation and planning as we had to mobilise the shielding response within one week. Daily tracking as performed to make sure deliverables were achieved.

Detailed findings

2. Shielding Citizens Contact and Driver Certification

Observations

Review of the processes applied to contact shielding citizens who had not already contacted the Council, and identification of drivers to support delivery of medical supplies highlighted a number of areas for improvement.

It is important to note that completion of outbound calls to shielding citizens did not identify any instances where citizens that were unable to contact the Council to request help had support needs that were not met.

1. Contacting Shielding Citizens

a) The timeline applied by the Council to contact shielding citizens was as follows:

- **Initial Interpretation** - the Programme board interpreted published Scottish Government (SG) guidance as allocating responsibility to NHS General Practitioners (GPs) to contact shielded citizens. Consequently, no contact was made by the Council with shielding citizens who had not already contacted the Council to request support between 9 April and 2 June when outbound calls commenced.
- **Clarification from SG** was received 15 May confirming the requirement for the Council to contact all shielding citizens who had not previously been in touch to request support.
- **Data Cleansing** was performed to identify all shielding citizens who had not already contacted the Council (circa 10,500 citizens). This was completed by 1 June.
- **Outbound Calls** commenced 2 June and concluded by 3 July 2020.

b) Completeness of Verint System Shielding Records – the manual reconciliation performed between the Verint Customer Relationship Management system records and SG shielding data identified a total of 33 shielding records that did not have a Covid-19 status flag applied due to missing address details. Management has confirmed that these citizens were not contacted as part of the outbound calling process.

c) The Risk Register was not updated to reflect the Council's responsibilities for contacting shielding citizens, and actions to be implemented to ensure that this was achieved following receipt of SG clarification in May

2. Protection of Vulnerable Groups Confirmation for Council Drivers

Review of Programme board papers confirmed that circa 100 existing Council drivers were identified with existing Protection of Vulnerable Groups (PVG) / Disclosure Scotland certificates to support delivery of medication to citizens, however, no evidence is available to support the confirmation obtained by the Programme to confirm current PVG validity.

Recommendations

In the event that the shielding and vulnerable groups programme is reinstated either in response to Scottish Government requirements; the Council's response to Covid-19; or if a similar programme is implemented in response to a future resilience incident, it is recommended that the Programme:

1. Immediately identifies areas where the published guidance is unclear and obtains clarification in relation to the requirement and implementation urgency, as highlighted in finding 1.
2. Ensures that the risks associated with any areas of uncertainty are defined; assessed; and recorded in the Programme risk register, together with action being taken to obtain appropriate clarification.
3. Considers reallocation of appropriately skilled resources from other services (where required) when clarification is received and there is an urgent need to prioritise and complete the task
4. Implements appropriate data quality checks to ensure that all records are complete with no missing data, and appropriate status flags are applied.
5. Where specific certification is required to support certain tasks (for example PVG certification to support delivery of medication), the requirement to confirm current validity should be recorded as a risk and considered. Where management decides that reliance will be placed on existing and historic records, this should be recorded as a Programme decision.

Risks

The potential risks associated with our findings are:

- **Public safety risk** – risk that the needs of shielding individuals who had not contacted the Council between 27 March 2020 (the date shielding lists and letters were issued by the NHS) and 2 June / 3 July 2020 were not identified and supported.
- **Public Safety Risk -** risk that drivers transporting medical supplies to citizens may not have a current and valid PVG status,

Management Comments

1. Some of the delay was to enable discussion with the Scottish Government in relation to the potential fraud risk associated with outbound calls.
2. Reliance was place on established Council PVG processes an assumption made (in the interests of time) that all drivers had a valid PVG.

Detailed findings

3. Third Party Support and Oversight Arrangements

Observations

Review of third party arrangements and Memorandums of Understanding (MOUs) established with the Edinburgh Voluntary Organisations' Council (EVOC) and Volunteer Edinburgh (VE) to support the Council's vulnerable groups (VG) response confirmed that:

1. **MOU documentation - t**here was no final signed copy of the VE and EVOC MOUs available in Board papers, and the final version of the EVOC MOU had no appendices attached to the final document, although these were referred to in the main document.
2. **Relationship Management and Oversight -** no single point of contact was established in the Programme to manage the relationships with and provide oversight of activities delivered by third parties in line with the agreed arrangements set out in the MOUs.
3. **Relationship Management and Oversight –** review of Board minutes confirmed that both EVOC and VE representatives attended the Board to provide progress updates and discuss issues, however the EVOC key performance report was discussed at a sub group that was separate from the main board with no formal updates provided by the sub group to the main board to confirm that performance had been discussed and any issues identified were resolved.
4. **Data Protection –** the data protection paragraphs in the MOUs do not specify what data must be returned to the Council by both voluntary organisations.
5. **Data Protection** – the MOUs did not clearly specify that third parties should complete data privacy impact assessments and would be data controllers as part of the VG support arrangements.
6. **Health and Safety** – the requirement to apply appropriate health and safety measures was specified in MOUs, but they did not include details of the nature of safety measures to be applied. Additionally, third parties were not requested to provide assurance to the board on the adequacy of safety measures implemented.

Recommendations

In the event that the shielding and vulnerable groups programme is reinstated either in response to Scottish Government requirements; the Council's response to Covid-19; or if a similar programme is implemented in response to a future resilience incident, it is recommended that the Programme:

1. Ensures that final signed versions of MOUs (or other equivalent documents) are approved by the Board and retained with Board papers.
2. Establishes a single point of contact to manage relationships with and provide oversight of activities delivered by third parties in line with agreed arrangements, who ensures that the Board is made aware of any significant issues and receive regular progress updates.
3. Ensures that appropriate arrangements are established for the secure return of any relevant data owned by the Council. **Note: it is important to ensure that both EVOC and VE are contacted and requested to return relevant VG data to the Council where the Council is the data owner and controller.**
4. Ensures that MOUs (or other equivalent documents) clearly specify where data privacy impact assessments should be completed and data controller responsibilities.
5. Ensures that detailed health and safety measures and ongoing assurance requirements are specified and agreed with third parties (especially where there is a potentially significant risk to public health).

Risks

The potential risks associated with our findings are:

- **Reputational Risk –** risk that third parties cannot be held to account where agreed services / support is not delivered effectively if there is no signed MOU.
- **Reputational Risk** – Inability to effectively monitor delivery of third party services / support and ensure that significant issues are identified, escalated and resolved.
- **Data Capture, Management and Use –** risk of non compliance with applicable Data Protection legislation where data recording; processing; management; ownership and use is not clearly specified in third party MOUs.
- **Data Capture, Management and Use –** risk of inappropriate retention and / or destruction of data owned by the Council by third parties.
- **Public Safety Risk –** risk that third parties do not establish and / or do not consistently apply appropriate health and safety measures when providing services to support the Council.

Management Comments

1. A signed version of the MOU was obtained for EVOC, but not for VE. Work on these documents was completed by the contracts / commissioning, legal and finance teams. Will check with authors from these areas whether signed versions complete with appendices are available.
2. Scottish expectation was that a reasonable level of oversight was required. Due to capacity challenges, circa two to three thousand people in Edinburgh were receiving food parcels from the third sector before the Council established its support processes. Complex negotiations had taken place to enable allocation and use of funding by the third sector, and additional time spent on oversight would have resulted in delays issuing food parcels.
3. Acknowledge that different approaches were applied to the review of third sector performance reports.
4. Agree that these could have been improved as there was no clear sense of what information was required to support delivery of the task.
5. Completion of DPIAs by third sector organisations was not considered a priority due to time and resource constraints.
6. Agree that there was no explicit follow-up performed by the Council to confirm that appropriate health and safety measures had been applied to volunteers.

Appendix 1

Basis of our classifications

Finding Rating	Assessment Rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation of the Council which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation of the Council.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the Council.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the Council. •

EQA
Setting the standards together

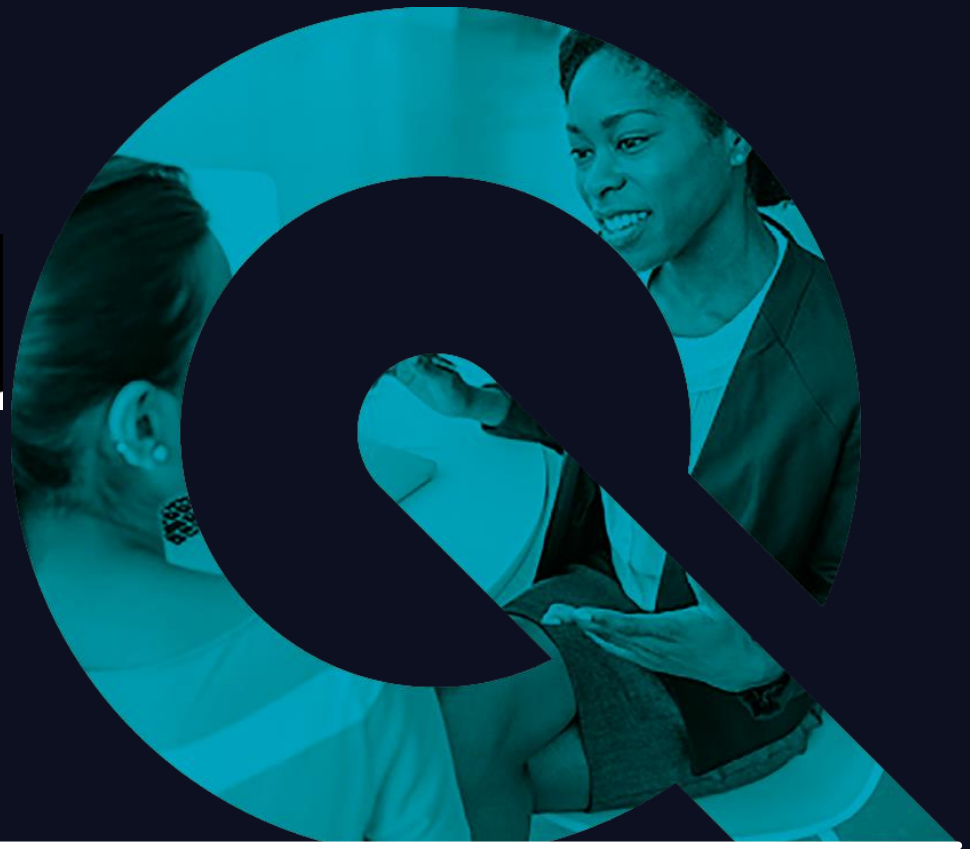
Chartered Institute of Internal Auditors

Review of the Effectiveness of Scrutiny of Governance, Risk and Best Value Committee

Report for:

Edinburgh City Council

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL



Prepared by Claire Ashby
The Chartered Institute of Internal Auditors

02 August 2021

Table of Contents

1 Executive Summary

1.1 Background, Scope and Approach

The City of Edinburgh Council appointed the Chartered Institute of Internal Auditors UK and Ireland ("the Chartered IIA") to undertake a review of the effectiveness of the scrutiny applied by the Council's Governance, Risk and Best Value (GRBV) Committee. This review forms part of the Council's internal audit programme. The Internal audit team is involved in the workings of the GRBV and therefore was not able to independently undertake this review. Therefore, the Chartered IIA were appointed as independent and objective reviewers.

The objectives of this review were:

- To provide an opinion on the effectiveness of the scrutiny applied by the GRBV, and
- To identify any areas for improvements in the arrangements of the Committee and raise associated recommendations.

The review approach has involved interviews with selected members and Council officers supported by a wider survey of members and heads of divisions, observation of GRBV meetings and review of GRBV papers, agendas and other records.

The Council's governance structure includes: the main Council and five Executive Committees (focused on activity areas e.g. Finance and Resources, Housing, Homelessness and Fair work) who have delegated decision making and scrutiny authority in relation to their area. GRBV has delegated authority to scrutinise the Council's governance, risk and best value arrangements. This includes monitoring financial and operational performance, whistleblowing and internal and external audit findings. The GRBV fulfils the role of the Council's audit and risk committee.

1.2 Conclusion

In regard to GRBV's responsibilities, as set out in its terms of reference, the Committee is fulfilling its core remit, particularly in relation to oversight of the internal and external audit processes, risk management and the operational performance of the Council. However, the current design of the arrangements for GRBV, do limit the effectiveness of the scrutiny it undertakes and the impact it can achieve.

The GRBV is to some degree constrained by the overall design of the Council's scrutiny model and we have made some suggestions for consideration when this model is reviewed post the 2022 elections.

Nevertheless, there are actions that could be taken, independently in relation to GRBV, which would enhance the Committee's effectiveness. We have made a number of recommendations in this regard. Some of these actions, such as considering adding independent experts to the GRBV, could be taken in the short term before the May 2022 elections.

1.3 Headline Findings

Both the Executive Committees and GRBV have delegated authority in relation to scrutiny. Some aspects of the effectiveness of GRBV can only be considered in the context of the full scrutiny model of the Council (of which GRBV is part). This wider scrutiny model was not within the remit of this review. However, much feedback was provided on this topic. Therefore, where supported by significant feedback and examples, relevant observations are set out in this report. These observations are for consideration when the Council's governance's structures are reviewed post the May 2022 elections. Particular consideration should be given as to whether the Council would benefit from an audit and risk committee with some independent experts sitting alongside elected members, as is common practice in other Councils. Independent experts supplement member skill sets and help address the perception of political motivations as described below.

There is also a need to review the relative scrutiny remits of GRBV and the Executive Committees. Whilst these remits are documented in terms of reference, in practice, there is a need for greater clarity and understanding by members of the alignment of scrutiny responsibilities.

Within the current scrutiny model, there are opportunities to enhance the effectiveness of the scrutiny undertaken by GRBV.

The key areas for attention include:

- Addressing the perception that the Committee is politically motivated in its activities. This was a significant area of feedback which is subjective in nature and therefore on which this review has not sought to draw a conclusion. However, even the perception of political bias has the ability to undermine the work of GRBV. Re-establishing the Vice Convenor role on GRBV (from a different political party to the Convenor) and considering the appointment of independent experts (see below) may aid in this regard.
- Considering ways to enhance the expertise and skills available to GRBV in relation to the audit, risk management and financial aspects of its remit. This could be achieved through a combination of improvements to training, skills assessments to inform appointments and the right of GRBV to appoint independent experts to support its work.
- GRBV taking time to stand back from its busy agenda, which is populated with an established routine of business, to consider its specific scrutiny goals and objectives for the year. These objectives should then inform its annual agenda. GRBV may wish to revisit the balance of focus on strategic and operational matters and its scrutiny activities focused on the outcomes/impact of Council policies. There is also an opportunity for GRBV to highlight good practice, as well as lessons learnt across the Council's activities.
- GRBV undertaking an annual effectiveness review against its objectives and publishing a report setting out its key observations and recommendations from its activities.
- Revisiting the referral process by which GRBV matters are passed to the Executive Committees for consideration. The Convenors of all the Committees involved could agree a protocol for such referrals setting out the criteria, information and guidance to be provided.

Our detailed findings are set out on the following pages including:

- A SWOT analysis of the GRBV.
- Findings and recommendations for each area of the review scope.

2 SWOT Analysis

What works well (Strengths)	What could be done better (Weaknesses)
• The Convenor post is held by the opposition. • Strong and widely respected Convenor. • Separation of GRBV membership from the Executive Committee Convenors. • Scrutiny of core remit areas including the annual accounts, whistleblowing, external and internal audit. • Attendance of senior Council officers (including S95 officer). • Transparency of GRBV activities (including webcasting of meetings). • Administration of the Committee (agenda setting, pre-meets and papers).	• Ensuring members (both on GRBV and on Executive Committees) are clear on the respective scrutiny roles of GRBV and the Executive Committees. • Ensuring GRBV has sufficient relevant skills amongst its members to fulfil the Committee's remit. • Member's training. • Application of the referral process. • Formalise the process for substituting for GRBV members. • More concise, focused papers.
What could deliver further value (Opportunities)	**What could stand in your way (Threats)**
• Annual consideration of the goals and objectives of GRBV by members. • Reviewing the work plan against the annual goals and objectives. • Producing an annual report of GRBV achievements/impact and key recommendations arising from its work. • Undertaking an annual self-assessment of effectiveness. • Undertaking a skills audit, using the results to create a skills matrix and advise groups on desirable skills to inform appointments. • Reviewing the balance of strategic and operational matters subject to scrutiny. • Post May 2022, re-considering the overall scrutiny model for the Council. • Considering the use of independent, expert members to augment GRBV skills.	• The perception that the Committee is driven by political motivation. • A limited pool of members with relevant skills willing or eligible to serve on GRBV. • Too frequent turnover of members. • Being overly focused on detailed operational matters (for example internal audit plans and findings) at the expense of strategic, big picture items. • Attempting to cover too many topics/areas in depth leading to packed agendas (whilst acknowledging that this is a reflection of the busy workplan of the Council).

3 Findings by Scope Objectives

3.1 Areas of Good Practice

The areas considered by the review are set out in Appendix 1. Positive findings were noted in relation to:

- **Culture of GRBV** - Whilst highlighting there can be occasional exceptions, most stakeholders commented that the culture of GRBV is appropriate. It is noted that a review of the member / officer protocol is currently being undertaken by the Council.

- **The administration the GRBV's business and activities** - There is efficient administration of GRBV's business including the timely issuing of papers and agenda planning meetings. No findings were noted in regard to this scope area.

The findings in relation to the remaining scope areas, and related recommendations, are provided below.

3.2 Management Responses

Management responses have been informed from elected member responses from a workshop attended by six GRBV elected members held on 23 June 2021.

3 Findings by Scope Objectives

3.3 GRBV Remit and Responsibilities

This section of the report sets out the findings in relation to the review objectives:

- The positioning, remit and responsibilities of the GRBV.
- The alignment and clarity of scrutiny responsibilities between GRBV and other Council bodies / Committees.

GRBV has a terms of reference setting out its remit and responsibilities. Many areas of its responsibilities are clear to all stakeholders such as review of the annual accounts, whistleblowing and oversight of internal and external audit. However, many interviewees cited a lack of clarity over the purpose of GRBV as a limitation in its effectiveness. In our survey, on a scale of 1 to 5 (where 1 is strongly disagree and 5 is strongly agree) 50% of member responses to the question “GRBV’s role and responsibilities are clear” scored 3 and below. This indicates there is a need to clarify the remit and responsibilities of GRBV.

The following matters were noted in regard to the remit and responsibilities of GRBV:

- **Perceptions of Political Motivation** – Much of the feedback regarding GRBV related to comments on the role of politics within the Council’s scrutiny model. The GRBV Convenor is rightly a member of the opposition. Many interviewees felt that GRBV’s activities are politically motivated whilst others did not feel this was the case. This is a subjective area. Therefore, this review cannot draw a conclusion and it would not be appropriate to do so. Regardless of the position, the perception by many stakeholders that politics is a key driver in scrutiny activities does impact on the effectiveness of GRBV. In particular, the attention given to GRBV’s referrals to other Committees. Therefore, it is recommended that consideration is given to measures that could reduce the perception of political bias within the scrutiny arrangements for GRBV.
- **The Council’s overall scrutiny model** - The Executive Committees also have a scrutiny role within their remit as defined within their terms of reference. The scope of this review did not include consideration of the scrutiny role of these Committees. However, many stakeholders have provided feedback that it is difficult to consider the effectiveness of GRBV without reference to the overall scrutiny model of the Council. At a high level, the current scrutiny model focuses the attention of the Executive Committee on scrutiny at the point policies and strategy are approved for implementation i.e. forward looking. This compares to GRBV’s post implementation focus i.e. backward looking. The alignment of these respective remits is critical in considering the effectiveness of scrutiny for the Council as a whole.

  Interviewees have provided examples of scrutiny models used by other Councils. It is understood other models were considered when the Committee structure was established in 2018 and the Council approved the current mode

3 Findings by Scope Objectives

Recommendations	Rating	Response & action date
1 When the Council's committee structure is designed in 2022, following the election, consideration could be given to: • Re-instating the role of Vice Convenor on GRBV with this position allocated to another (non-administration) political party. • Independent experts joining GRBV as non-voting members (see section 3.21 below on skills). • A cabinet structure with each Executive Committee having a scrutiny oversight Committee. • The inclusion of an Audit and Risk Committee within the Committee's structure. • Independent experts being included in the membership of such a committee would help ensure the quality of scrutiny over key areas such as the annual accounts.	**Medium**	1.1 The Council usually reviews its political management arrangements in the weeks and months after an election. Consideration will be given at that time to a range of models, including a cabinet model. This review will consider how the GRBV committee is constituted and its remit for governance across the Council. The use of a vice convener and the introduction of independent members for the audit and scrutiny committee will also be considered at that time. Ultimately, it must be recognised that the Council will determine which committee structure is implemented, regardless of officer recommendations. When determining the potential future structure of the committee, it is important to remember that GRBV is a Council committee and that elected members have overall responsibility for scrutiny. **16th December 2022** 1.2 In the interim, officers in consultation with relevant conveners will prepare a briefing note for all councillors setting out the Council's current scrutiny process. **17th December 2021**

- **Work Programme of GRBV** – There are opportunities to enhance the clarity of purpose of GRBV within the current structure without addressing the two points above. For example, there are opportunities to revisit the annual plan of work for GRBV to ensure it is focusing attention on the most important scrutiny topics. The annual work plan has been developed overtime and leads to a full agenda of meetings throughout the year. There is a risk that GRBV is overly driven by the established work plan, derived from

3 Findings by Scope Objectives

historic activity, without taking the time to stand back and consider its objectives and goals for any given year within the context of the Council's wider work programme.

In reviewing GRBV's work plan, it is noted that the Committee is often focused on detailed operational matters. This is partly driven by its role in scrutinising internal audit findings on the Council's policy and procedure framework. Few examples were observed where GRBV focused attention at a strategic level. This partly reflects the previous finding regarding the need to ensure alignment and understanding of scrutiny throughout the Council's Committee structure. However, independently GRBV has the opportunity to consider its focus on strategic activities such as the delivery of the Council's business plan.

Two further points were noted in regard to GRBV's work programme:

- There is an opportunity for GRBV to increase its focus on the outcomes and impact of Council policies (versus the operational processes within the Council).
- The role of GRBV in highlighting "good news stories" and positive findings in relation to the Council's activities.

Recommendations	Rating	Response & action date
2 Annually GRBV should set a series of objectives and goals for its scrutiny activities during the financial year (which are then evaluated at year end – see (3) below).	**Medium**	2.1 It is proposed to hold a workshop with committee members and key officers to determine GRBV's goals and objectives at the beginning of the new Council. This review will also consider whether a strategic focus for the Committee could potentially result in an increased perception of politicisation of the committee. he effectiveness of the process will be reviewed at the end of the year to confirm whether this or an adapted model should continue for future years. **16th December 2023** 2.2 In the interim officers and committee members will prepare a lessons learnt paper that captures the lessons learnt relating to GRBV from this iteration of the Council. **27th May 2022**

3.4 The Skills and Resources available to the GRBV

3.4.1 Expertise of Committee members

The skills available to GRBV was also an area of significant feedback. Integral to the Council's governance arrangements is the democratic composition of its Committees. Therefore, GRBV is rightly comprised of members. Stakeholders did though provide feedback that the technical and specialist nature of many aspects of GRBV's business demands that GRBV is supported with the requiste skills to ensure the quality of questioning and ultimately the quality of scrutiny. In our surveys, 63% of elected member respondees and 68% of heads of management respondees scored 3 or lower the statement "GRBV has adequate skills and expertise to fulfill its remit" (where 1 is strongly disagree and 5 is strongly agree). This aligns with our observation that there is scope to enhance the skill set of GRBV.

Risk management, financial and audit expertise is of particular benefit to GRBV due to its remit in these areas. Only a small number of current members have expertise in these fields. Where this expertise sits within the opposition party, this lends weight to the perception (correct or otherwise) that the questioning of the GRBV members is politically motivated. Some stakeholders also highlighted that as the quality of the internal audit service has developed, the expertise required by GRBV to oversee the internal audit findings needs to be strengthened.

GRBV has not previously undertaken a skills assessment to identify the expertise it requires, the skills fulfilled by current members and skills gaps. Such an exercise may be beneficial in identifying skills gaps to inform the future members appointed by Council political groups. The current GRBV terms of reference does not allow for independent experts to join the committee (as a non voting member) or for GRBV to appoint independent experts to assist on particular topics. Both these options could bring benefits by enhancing GRBV's skill set.

Recommendations	Rating	Response & action date
3. An annual skills assessment should be undertaken by GRBV. The results should be provided to the political groups to inform appointment of members.	**Medium**	It is proposed that we work with elected members in the new Council to identify skills and experience. This can then be provided to political groups to aid all appointments to committees and ALEOs. This skills audit can then be regularly updated. A self-assessment exercise will be carried out in early 2022 with the executive committees and GRBV which will inform the skills needed for each committee. **30th September 2022**

4. When the Council's Committee structure is reviewed post the 2022 elections, following the elections, consideration could be given to the GRBV terms of reference: • Allowing for the appointment of independent non-voting members with requisite skills. • Allowing the Committee to appoint independent expertise to advise on specific matters.	**Medium**	The Council usually reviews its political management arrangements in the weeks and months after an election. Consideration will include an option to appoint independent non-voting members to GRBV or its successor. This process will involve considering how the appointment of independent non-voting members and / or independent expertise could work in practice, and also any associated financial implications. **16th December 2022**

3.4.2 Training for Members

There are opportunities to enhance the training provided to GRBV members. Training is delivered to members by the internal and external auditors. The following points were noted in regard to this:

- The training provides useful information on risk management, internal audit and external audit. However, it does not cover all aspects of GRBV's remit and the wider scrutiny model of the Council.
- Whilst the training is offered on appointment, there is no requirement for members to attend. When political groups change their GRBV appointed members, there is no mechanism to ensure the new members are offerred the training. Section 7.4 of the GRBV terms of reference states that "substitutes are permitted…..who have undertaken and completed appropriate training as specificed by the Chief Executive". However, in practice there is no monitoring of whether GRBV members or substitutes have completed relevant training.

- The GRBV Convenor does not receive any additional training in respect of their role. They are in effect the Chair of the Audit & Risk Committee and as such there is technical training which could be beneficial to this individual.

- Members also commented that:
  - They could not recall whether or not they had received training;

3 Findings by Scope Objectives

- That training was provided soon after appointment when there was a large volume of information to assilmate and individuals were not yet familiar with their roles. The latter resulted in limited appreciation of the relevance of the training being provided.
- For some members, the areas of audit and risk management were entirely new to them and more support was needed to ensure they were suitably equipped to fulfil their scrutiny responsiblities.
- There was a need for refresher training during the term of appointment and training on specific topics.

Recommendations	Rating	Response & action date
5. The Governance team are currently reviewing members' training arrangements. For the 2022 appointments, consideration should be given to: • The phasing of training over a longer period to allow an understanding of individual's roles to firstly develop. • Mandatory training requirements for GRBV members. • Refresher and specialist topic training being provided during the term of appointment. • Specific training for the GRBV Convenor in respective of the technical aspects of their role e.g. attending external training on the role of an Audit and Risk Committee Chair.	**Medium**	5.1 Consideration will be given to all of the recommendations as part of the review of elected member training. The phasing of training is a perennial issue and a balance between getting elected members ready quickly for their duties and that being phased to allow for greater understanding is a key consideration. Specific training for the Convener can be brought in and some refresher and specialist training is carried out over the term, but a more robust programme will be explored. **28th October 2022** 5.2 In the interim, training will be arranged prior to the presentation of the Internal Audit annual opinion and the audited financial statements. **29th October 2021**

3.4.3 Deputising for Members

There is no formal deputising process for when appointed members are not available to attend meetings. One political party rotates its attendance at GRBV amongst its members. These points, along with a turnover of members and lack of mandatory training requirements, can lead to members attending who do not have the knowledge of GRBV's annual agenda and historic activities. This poses a significant risk to the quality of questions and GRBV's overall effectiveness.

Recommendations	Rating	Response & action date
6. A formal deputising process with set requirements (e.g. completion of mandatory training, understanding of the annual agenda and the goals and objectives for the year) should be established.	**Medium**	This was put into place in the previous Council term but was never sustained. All members would be invited to attend the required training, but it is not proposed that a firm approach is taken to substitute members having attended the required training **Risk Accepted**

3.5 The Effective Execution of the GRBV's Responsibilities.

3.5.1 Annual Review of Effectiveness

There is currently no mechanism for GRBV to annually consider and report on its effectiveness. It is good practice to undertake such an review. This would also provide an opportunity for GRBV to set out its key observations and recommendations for the Council arising from its year's work.

Recommendations	Rating	Response & action date
7. GRBV should undertake an annual effectiveness review against its objectives and goals for the year. This should inform an annual report of its activities	**Medium**	This will be incorporated into the self-assessment review of committees in 2022 and then will be part of the committee's annual workplan after the Local Government Elections in 2022.

highlighting key observations (including positive achievements) and recommendations for the Council.		**29th September 2023.**

3.6 The operation of the GRBV's meetings and activities

3.6.1 Referral Process

Where GRBV deem it appropriate, the Committee refers reports to the Executive Committees. There are opportunities to enhance the effectiveness of the referral process with the following points noted:

- Feedback has been received that the purpose of these referral is not clear. A review of a sample of recent referrals suggests the purpose of the referrals and action recommended to the receiving Executive Committee could be more clearly articulated via a covering note.
- The timing of meetings means that referrals can be received by Executive Committees up to three months after they have been referred by GRBV. This means that the related report may be out of date by the time it is tabled. This is particular issue for the referral of outstanding management actions arising from audits.

Red rated internal audit findings are received by the respective Executive Committee after they have been tabled at GRBV (lower rated findings are not seen by the Executive Committee). There is an argument that such issues should be immediately highlighted to the respective Executive Committee for oversight (regardless of GRBV referral) in line with Executive Committees' scrutiny roles. An immediate referral would also avoid delays in the receipt of the findings

Recommendations	Rating	Response & action date
8. The GRBV Convenor should agree a protocol with the Executive Committee Convenors for the referral of items from GRBV. This protocol should set out the information which is required to ensure that the referral process works effectively e.g., the specific matters within the report which require attention, the actions	**Medium**	A protocol for referred items will be drafted following discussions with relevant conveners. This will include provision of covering notes with referral reports that indicate what specific action is required by executive committees and details of any subsequent updates required by GRBV and take account of any additional resource impacts on the Internal Audit team.. **17th December 2021**

	recommended to the Executive Committee by GRBV, in relation to the referral.		
9.	The referral process should be reviewed to ensure only up to date information is referred in relation to internal audit actions and findings. This could involve: • Red audit findings being immediately referred to the Executive Committees by Internal Audit prior to tabling at GRBV (it is accepted that IA would not have resource to attend all meetings). • Directorates preparing their own updates on the status of internal audit actions for the Executive Committees. The Council wide view would then be presented by Internal Audit at GRBV.	**Medium**	A protocol for referred items will be drafted following discussions with relevant conveners. **17th December 2021**

3.6.2 Other Operational Matters

Two, lower rated points were also noted in relation to the operation of GRBV:

- The volume and detail within the papers can inhibit the ability of members to review all the information provided.
- Meetings can be overly length. The agenda does not include the timings of each agenda item to indicate its importance within the overall meeting.

Recommendations	Rating	Response & action date
10. GRBV could provide further direction to Council Officers in regard to the level of detail the Committee would like included with the papers.	**Low**	Reporting to committees will be part of the review of political management arrangements and councillors will be able to feed into that process. **16th December 2022**
11 Consideration could be given to assigning timings to each agenda item.	**Low**	This has been tried before and has not been successful due to it not being enforceable. It is not recommended that this is pursued. **Risk Accepted**

A1 Review Scope

Scope Areas

The following matters were within the scope of this review

- The positioning, remit and responsibilities of the GRBV.
- The alignment and clarity of scrutiny responsibilities between the GRBV and other Council bodies / Committees.The skills and resources available to the GRBV.
- The effective execution of the GRBV's responsibilities.
- The culture of the GRBV, ethics and conflict of interest arrangements.
- The administration of the GRBV's business.
- The operation of the GRBV's meetings and activities.

Scope Exclusions

This review is solely focused on activities of the GRBV and not the wider governance arrangements of the Council.

The ethical and conflict of interest arrangements for GRBV have not been reviewed in detail. No related issues came to our attention. Whilst originally within the review scope, it was noted that these are Council wide procedures covered elsewhere by internal audit.

A2 Review Approach

Documentation Review

Review of GRBV terms of reference, agendas and papers

Observation

Observations of GRBV meetings via the webcast recordings of meetings

Interviews

Feedback from elected members and Council officers via 1:1 interviews (see below for details)

Surveys

Feedback from a wider pool of stakeholders via surveys of (1) all elected members of GRBV (2) “heads of” management group

Stakeholder Interviews

The following individuals were interviewed as part of the review.

One GRBV member per political party was randomly selected by the Chartered IIA for interview. A meeting was also held with the Convenors of a sample of Executive Committees.

Members	Title / position	Council Officers	Title / position
Eleanor Bird	Elected Member	Hugh Dunn	Head of Finance
Kate Campbell	Convenor of Housing, Homelessness and Fair Work Committees	Andrew Kerr	Chief Executive
Phil Doggart	Elected Member	Gavin King	Democracy, Governance and Resilience Senior Manager
Gillian Goyer	Elected Member	Paul Lawrence	Director of Place
Lesley Macinnes	Convenor of the Transport and Environment Committee	Stephen Moir	Director of Resources
Adam McVey	Council Leader	Lesley Newall	Chief Internal Auditor
Joanne Mowat	Convenor of the GRBV	Judith Proctor	Executive Director of Health & Social Care
Gordon Munro	Elected Member	Nick Smith	Head of Legal and Risk
Susan Rae	Elected Member	**Other**	
Donald Wilson	Convenor of the Culture and Communities Committee	Nick Bennet and Karen Jones	Azets (External Auditors)

Acknowledgement

We would like to thank all Edinburgh Council members and officers for their assistance and support during this review including their open and honest views.

A3

Basis of Classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation of the Council which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation of the Council.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the Council.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the Council.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

A4 Elected member Workshop Outcomes

Purpose of meeting

An Audit of the Effectiveness of GRBV Committee has been carried out as part of the Council's Audit programme. This was carried out by Clare Ashby on behalf of the Chartered Institute of Internal Auditors. The purpose of the meeting was to provide a Committee response to the draft Internal Audit which will feed into the Management response.

Overall feedback

Overall, those at the meeting (the Meeting) felt that the report was fair and the following responses were agreed

A4 Elected member Workshop Outcomes

Scrutiny – Recommendations 1; 8; 9 Clarity of respective scrutiny roles of GRBV and Executive Committees – it was accepted that the process doesn't seem to be clearly understood and the Convener proposed that a paper was written setting out the process and how it should work for circulation to address the immediate issue. It would be helpful for officers to present the overdue Audit report by Executive Committee, so it is easier to split out the relevant area for presentation to Committees. A clearer covering note should be attached. Actions: 1. Officers and Convener to prepare a briefing note setting out current process and improvements required. 2. Covering notes attached to referral reports should indicate specific action required and what reporting back expected.	**Training - Recommendation 5** The need for training identified was a fair finding and the Meeting were enthusiastic about initial and continual training and felt that this was an action that should be picked up with some urgency. Specifically, they would welcome training/external advice prior to the Audited accounts being presented later this year and there should be discussion with Committee about what the training needs were. Actions: 1. Training arranged prior to presentation of Audited Accounts. 2. Training needs audit for Committee to be carried out.
Annual Work Plan and Report – Recommendation 2 The Meeting agreed that having an annual work plan and report was desirable – not only for GRBV but for all Committees, however it was felt that within the current SO and TOR this would be difficult to achieve and should be given consideration for the next iteration of the Council. Action: 1. Officers and Committee should prepare a What worked well/ What could be done better paper for the next iteration of the Council to capture the learning of this session of Council.	

A4 Elected member Workshop Outcomes

Independent Experts and Skills – Recommendations 1; 3; and 4 On the suggestion that there should be external members of the committee the Meeting felt that membership of the Committee would require more thought about how this would work. Some present were concerned that the external qualified members might make the Councillor members feel less responsible when this is, and always should be a Council committee. Concerns raised how many external members might be needed to plug any skills gap identified and it was agreed that external input would be welcome and useful but that at this stage membership of the Committee would be difficult to achieve and access to expertise would be preferable in the first instance and welcomed by the Committee. Action: 1. Identify skills gaps in the current Committee membership.	**Strategic Focus - Recommendations 2 and 4** Concern was expressed about whether in a political environment moving out of the operational sphere to focus on the strategic wouldn't lead to more concerns about the politicisation of the Committee. Whilst the Meeting expressed an interest in doing this there is a requirement for there to be an "apolitical" arena in which scrutiny of the management effectiveness of the Council can take place so that the focus is on whether management is or can deliver. There would need to be a robust suite of SMART, and unambiguous measures, to permit this and it is unclear that this could happen in a political environment. The Meeting felt that as the new Business Plan is developed and comes into force there may be areas of this that can be assessed against criteria but this is a complicated piece of work and the Meeting felt that this should be captured as a recommendation for the wider piece on how scrutiny is done post 2022. This is interlinked with the perception of political bias – as that perception appears to exist in some areas of the Council it was felt that it would undermine the work of the Committee to look to move to a remit that could easily become more politicised. The place in the electoral cycle should also be considered as we respond to these concerns. It is of concern that this perception exists but with clarification of the remit of role of referrals it is hoped that this can be neutralised in the short term and that the longer term plans for the post 2022 piece can fully address this. Action: 1. Officers to include in the work looking at the post 2022 election and possible Governance arrangements options for scrutiny and how GRBV (or any successor Committee) is constituted and its remit within the wider role of the Governance of the Council.

Disclaimer: This review was undertaken in March and April 2021 by Claire Ashby on behalf of the Chartered Institute of Internal Auditors. This report provides the officers and the GRBV of Edinburgh Council with information about the effectiveness of scrutiny of GRBV as of that date. Future changes in environmental factors and actions taken to address recommendations may have an impact upon the effectiveness of scrutiny of GRBV in a manner that this report cannot anticipate.

Considerable professional judgment is involved in evaluating and reaching the conclusions of this review. Accordingly, it should be recognised that others could draw different conclusions. This report is provided on the basis that it is for your information only and that it will not be quoted or referred to, in whole or part, without the prior written consent of the Chartered Institute of Internal Auditors.

© Chartered Institute of Internal Auditors.

The City of Edinburgh Council

Internal Audit

Findings Only Report – Salary Overpayments

Final Report

11 June 2021

RES2009

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.

Contents

The Internal Audit Charter approved by the City of Edinburgh Council's Leadership Advisory Panel in March 2020 notes that Internal Audit also reserves the right to raise findings on areas that have not been specifically included in the annual plan where significant or systemic control gaps are evident.

This Internal Audit findings only review is conducted for the Council under the auspices of the 2020/21 Internal Audit Charter. The review is designed to help the 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 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 is a number of 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 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.

1. Background and Scope

Background

Following the issue of the final Employee Lifecycle Data and Compensation and Benefits Processes for the 2019/20 Financial Year Internal Audit (IA) report in December 2020, IA performed additional work on the management of employee salary deductions for employees with focus on recovery of salary overpayments.

Salary overpayments routinely occur for both current and formal employees due to delays in first line managers providing information to Human Resources (HR) when employees leave the organisation, or their current employment situation changes (for example the end acting up arrangements). They also occur (less frequently) due to HR processing errors.

Both manager responsibilities for submitting any information relating to a change in an employee's salary to HR before the payroll deadlines, and the rigorous processes that are applied where employees have been overpaid are detailed in the Council's pay policy that was approved at the February 2020 Policy and Sustainability Committee meeting.

The Council's Current Salary Overpayment Position

As at 12 February 2021, circa £1,250k is owed to the Council by 958 current or former employees. This equates to 0.23% of the cost of payroll to the Council in 2018/19 (£551m).

The Council's 2019/20 Annual Audit Report notes that external audit's assessment of financial materiality applied to the audit of the Council's 2019/20 financial statements was £19.8M, which confirms that the current overpayments position would not be considered material from an external audit perspective.

A dedicated HR team member was appointed in October 2020 to manage the process applied by HR to recover overpayments once identified. In addition, management has advised that:

- A data quality team, consisting of two Grade 6 members of staff, was introduced November 2021 to review processes, perform error checking, and perform training;
- The total overpayment balance reduced by £48,236 between February and March 2021; and
- The accuracy of payroll (based on the number of salary overpayments) was 99.11% for 2020-21. The average for the previous 8 months was 99.24%.

The following table summarises the position:

Analysis of salary overpayments as at 12 February 2021	Current Employees	Former Employees	Total
Current number of individuals who owe money	617	341	958
Current amount owed	£827,610.90	£422,482.40	£1,250,093.30
Number of letters issued to staff in order to commence the debt repayment process	525	266	791
Number of individuals with repayment plans in place	406	49	455

Total amount owed by individuals with repayment plans in place	£574,438.78	£75,368.90	£649,807.68
Number of individuals with no repayment plan in place	211	292	503
Total amount owed by individuals with no repayment plan in place	£253,172.12	£347,113.50	£600,285.62

HR Processes Applied

When a salary overpayment is identified by HR, or they have been informed by a line manager, a salary overpayments form is submitted through the AskHR portal. HR will then note the overpayment on the spreadsheet used to monitor all debts owed by current and former employees, and request details of any missing information from the relevant service.

When overpayments have been made to current employees, HR will contact the employee to inform them that the debt will be repaid through salary deductions that are commensurate with the employee's salary and do not require the employee's consent as detailed in the pay policy.

Where overpayments have to be recovered from former employees, the former staff member will receive a letter from HR outlining the amount owed and requesting engagement and agreement on suitable debt recovery arrangements. If a debt recovery arrangement cannot be agreed, then the former employee will be contacted by the Council's Accounts Receivable team who will again request agreement on appropriate debt recovery arrangements. Where this approach also fails then the debt will be passed to the Council's external debt recovery agency, incurring additional external costs.

All costs associated with salary overpayments (including debt recovery and write-offs) are recharged to relevant division and directorate budgets. HR has confirmed that no historic salary overpayments have yet been written off, and approval for all write-offs would be obtained from the Executive Director of Resources.

Scope

The Internal Audit Charter that was approved by the Council's Leadership Advisory Panel in March 2020 notes that Internal Audit reserves the right to raise findings on areas that have not been specifically included in the annual plan where significant or systemic control gaps are evident.

Reporting Date

Our audit work concluded on 12 February 2021 and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 1

Summary of findings raised	
High	1. Salary Overpayments

Opinion

Some Improvement Required (Amber)

Whilst some significant control weaknesses were identified in the design and effectiveness of the control environment and governance and risk management frameworks supporting identification and recovery of salary overpayments, they provide reasonable assurance that risks are being managed, and that the Council's objectives to ensure that employees are accurately paid for the work they have performed should be achieved.

Our 'Some Improvement Required' (Amber) overall report opinion is based on the fact that the total current value of overpayments (£1.25m) that have been identified would not be considered material by external audit; and the highest risk area where overpayments may not be recovered relates to former employees where no debt recovery plans have been established (currently 292 employees owing circa £347k).

It is important to note that whilst the current value of overpayments would not be considered material by external audit, it is essential that Council minimises any potential loss of income given the ongoing financial impacts of the Covid-19 pandemic, and the challenges associated with delivering a balanced outturn for 2020/21 and a balanced budget for financial year 2021/22.

Additionally, both first line management responsibility for submitting any information relating to a change in an employee's salary to HR before payroll deadlines, and the processes that are applied where employees have been overpaid, are clearly detailed in the Council's pay policy.

The High-rated finding included in the report reflects that first line managers are not consistently complying with the requirements to advise HR of any changes that could potentially affect the accuracy of salary payments; that no first line controls have been established to confirm that all employee changes are consistently advised to HR; and the opportunity for some improvement in the recovery processes applied by HR.

HR management has also confirmed that they were aware of the historic salary overpayment issues and have been working progressively to implement processes to ensure that they are addressed. This commenced in the later part of the 2020/21 financial year, and progress is evident with the approval of the new pay policy in February 2020; the temporary realignment of a dedicated HR FTE to manage the overpayments process; and planned process improvements that are aligned with the recommendations in this report.

It is acknowledged that progressive implementation of HR processes to address the historic salary overpayments position has taken time to implement due to reliance on manual intervention; manual processes (for example, a spreadsheet is used to manage overpayments which is a complex process); and HR capacity. It is also important to note that IA work performed in the Employee Lifecycle Data and Compensation and Benefits Processes for the 2019/20 Financial Year audit did not highlight the extent of payroll overpayments, as the audit applied use of data analytics to confirm whether payroll transactions were accurately based on employee payroll data maintained in the payroll (iTrent) system.

Use of data analytics did highlight a significant volume and value of non-statutory (PAYE; NI; and pensions) deductions that resulted in completion of further follow-up work and identification of the salary overpayments issue.

3. Detailed findings

1. Salary Overpayments — High

As at 12 February 2021, circa £1,250k is owed to the Council by 958 current or former employees. The total amount owed equates to the 0.23% of the cost of payroll to the Council in 2018/19 (£551m).

It was also noted that the debt recovery process has not yet started for 503 individuals (53% of the total), who owe over £600,000 (48% of the total amount owed). HR leadership has advised that letters were sent to all former employees who had been overpaid, and that this balance relates to those who have not yet responded where further action is required.

The largest debt incurred was for £36,141. The overpayment was to a staff member who had taken unpaid leave in August 2018, but had continued to receive a salary; HR had not been informed by the staff member's line manager. The error was identified when the staff member handed in their notice in May 2020. This debt is now being managed by the Council's debt recovery team.

The two oldest outstanding debts date back to 2010, with amounts of £8,201 and £5,481. Repayment plans for these two debts were put in place in 2017, and the amounts still owed are £5,221 and £881 respectively.

A review of the current process applied by HR to record, manage and recover salary overpayments established that:

1. the debt recovery process has not yet started for 503 current and former employees (53% of the total) who owe over £600,000 (48% of the total amount owed).
2. The pay policy states that where a pay error is deemed to have come about because of a service area's failure to meet deadlines (when they could have reasonably done so) a re-charge of £150 will be levied against the service area for each instance. HR leadership has confirmed that these recharges have yet to be applied, which is in line with the agreed implementation approach.
3. the spreadsheet used to manage the debt recovery process has a number of information gaps for some of the debts, for example, the date the overpayment occurred, the reason for the overpayment, the details on the nature of the overpayment, and the date the debt recovery letter was issued. HR leadership has advised that these issues are currently being addressed.
4. there are no details maintained of overpayments that could not be recovered and were written off.

Risks

The potential risks associated with our findings are:

- Potential loss and additional financial costs incurred by the Council in relation to external debt collection agencies or where overpayments are written off;
- Impact on the Council's liquidity and cash flow; and
- Resourcing impacts on both HR and the Council's debt management teams.

1.1 Recommendation – Human Resources management of overpayments

It is recommended that Human Resources:

1. Immediately initiates debt recovery processes for the 503 individuals who currently owe £600k in salary overpayments to the Council.
2. Implements application of the £150 recharges as detailed in the pay policy against relevant directorates and divisions.

3. Refreshes the overpayments spreadsheet to include details of the age of overpayments; their current status; the line manager responsible for the relevant employee; and any overpayments written off for all individual cases, and includes this information in the monthly updates provided to divisions and directorates.
4. Designs key performance measures or indicators in relation to salary overpayments at both top of Council and directorate level; agrees them with directorates; and requests their inclusion in the Council's new workforce dashboard.
5. Records the risks associated with the HR overpayments process in the HR risk register.

1.1 Agreed Management Action – Human Resources

1. As at 13th April there are 290 employees/former who have not responded to overpayment letters. These employees/former require channelled into the debt recovery process and invoiced, however as these are historical debts cost centres need reopened for this process to be fulfilled. We also have 150 employees who still require an initial communication. It is our intention to have this piece of work completed by the end of June 2021.
2. At this time and particularly in relation to the current pandemic situation and embedding different and flexible working practices across the Council it is not our intention to levy the £150 charge to service areas. We will however keep communicating with HOS and offering assistance where we see managers may need assistance with process.
3. We will review how we manage the overpayment data and information that is relevant can be included.
4. We can include the overpayment data as a key performance measure for directorates and the Council.
5. The risks are logged on the HR risk register not just in relation to manager compliance but also associated with the reliance on manual processes and spreadsheets and process complexity.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Lifecycle Lead Consultant; Laura Manson, Senior HR Adviser; Layla Smith, Operations manager, Resources; Michelle Vanhegan, Executive Assistant, Resources	**Implementation Date:** 30 October 2021

1.2 Recommendation – Directorates

It is recommended that directorates:

1. Implement appropriate controls to confirm that line managers have advised HR of all payroll changes in advance of the payroll cut-off date, for example by obtaining confirmation from all service managers that Payroll have been advised of all relevant changes.
2. Review the overpayments spreadsheet provided by HR, and ensure that recurring instances of failure to notify HR are addressed as part of ongoing performance management discussions.
3. Record the risks associated with significant and recurring salary overpayments in relevant divisional and directorate (where appropriate) risk registers.

1.2.1 Agreed Management Action – Place

1. A communication will be circulated to all third tier managers in the Place Directorate, for cascade through services areas to remind line managers of the importance of advising HR of all payroll changes in advance of the payroll cut-off date. Place will not request confirmation from service managers that Payroll have been advised of all relevant changes.

2. Place Senior Management Team will review the overpayments spreadsheet provided by HR and will take appropriate action to follow up on recurring instances of failure to notify HR, including where appropriate, this being addressed as part of ongoing performance management discussions.
3. Where appropriate, risks associated with significant and recurring salary overpayments will be recorded in relevant service area risk registers.

Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Head of Place Management; Michael Thain, Head of Place Development; Alison Coburn, Operations Manager	**Implementation Date:** 31 March 2022

1.2.2 Agreed Management Action – Health and Social Care Partnership

The Partnership will continue (through its reporting structures) to remind line managers to advise HR of all payroll changes. The Partnership will ensure that the overpayments spreadsheet is reviewed and appropriate actions will be taken where recurrent instances are happening.

Owner: Judith Proctor, Chief Officer (EHSCP) **Contributors:** Angela Ritchie, Operations Manager (EHSCP)	**Implementation Date:** 31 December 2021

1.2.3 Agreed Management Action – Strategy and Communications

Controls have been instituted to ensure that Senior Managers confirm each month that HR has been advised of all payroll changes for staff and elected members. The overpayments spreadsheet has been reviewed and associated risks have been added to the divisional risk register.

Owner: Andrew Kerr, Chief Executive **Contributors:** Andy Nichol, Programme Manager (PMO) Edinburgh and South East Scotland City Region Deal/Edinburgh 2050 City Vision; Gavin King, Democracy, Governance and Resilience Senior Manager; Gillie Severin, Strategic Change and Delivery Senior Manager; Paula McLeay, Policy and Insight Senior Manager; Michael Pinkerton, Senior Communications Manager	**Implementation Date:** 10 May 2021

1.2.4 Agreed Management Action – Communities and Families

Senior Managers will ensure that staff/workforce updates are included as a standing item at management team meetings and their service managers will oversee any changes within their team ensuring direct line managers are supported and aware of the Council's pay policy. Where there is reliance on colleagues from Resources who are aligned to divisions to provide support with HR functions, the responsibility for ensuring HR are advised of any changes sits with the service manager and line manager. A checklist, which includes timescales should be generated when a line manager is made aware by a direct report of anything which will impact on their pay, including notice to leave employment, these timescales will include dates for submitting information to HR to ensure payroll cut-off dates are taken into consideration.

Senior Managers will ensure that any instances of failure to notify HR, noted on the overpayments spreadsheet, will be investigated by the service manager and performance management measures implemented if necessary. Any service area which has recurring instances of failure to comply with pay policy will be flagged to HOS and highlighted in Team Briefs, Risk Matters or other comms. In the event of recurring overpayments within a division or the directorate, this will be included within risk registers with appropriate controls and actions noted.

Owner: Jackie Irvine, Head of Safer and Stronger Communities / Chief Social Work Officer	**Implementation Date:** 31 August 2021

Contributors: Nichola Dadds, Operations Manager (Communities and Families)	

1.2.5 Agreed Management Action – Resources	
A further communication will be issued to all Heads of Service and third-tier managers in the Resources Directorate by the Executive Director of Resources, for cascade through services areas to remind line managers of the importance of advising HR of all payroll changes in advance of the payroll cut-off date. Resources will not request confirmation from service managers that Payroll have been advised of all relevant changes because this would be overly onerous. Where appropriate, risks associated with significant and recurring salary overpayments will be recorded in relevant service area risk registers.	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Nicola Harvey, Head of Customer and Digital Services; Katy Miller, Head of Human Resources; Nick Smith, Head of Legal and Risk; Peter Watton, Head of Property and Facilities Management; Layla Smith, Resources Operations Manager and Michelle Vanhegan, Executive Assistant	**Implementation Date:** 30 September 2021

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***; or*** • ***Critical*** impact on the reputation of the organisation which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***; or*** • ***Significant*** impact on the reputation of the organisation.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the organisation.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Please see the Internal Audit Charter for full details of opinion ratings and classifications.

The City of Edinburgh Council

Internal Audit

Technology Resilience

Final Report

20th July 2021

[RES2006]

Overall report rating:

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.

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2020/21 internal audit plan approved by the Governance, Risk and Best Value Committee in September 2020. 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 a number of 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.

1. Background and Scope

Background

Technology resilience is defined as an organisation's ability to respond to and recover from service impacts of a severity that necessitates the use of replacement technology or transfer of operations to alternative premises, with restoration of technology systems in order of service criticality.

Technology's role in supporting service delivery is becoming increasingly critical and complex as organisations digitise and automate more services, with the likelihood of incidents and events that disrupt the delivery of these services increasing.

This highlights the importance of technology as a foundation pillar within a robust operational resilience framework, and reinforces the need for organisations to fully understand their key technology risks, criticality, and dependencies across the organisation to ensure effective recovery from service failures and disruptions.

Appendix 3 includes a high level overview of the key components of an operational resilience, and highlights the importance of technology in an operational resilience framework.

Definition of key terms

Within a technology resilience framework, the following definitions are applied:

- **BIA**: Business Impact Assessment (BIA) captures an organisation's understanding of the criticality of its business activities/services and their dependencies including systems, resources and third parties. This information is captured to ensure operational resilience and continuity of operations during and after a business disruption.
- **RTO**: The Recovery Time Objectives (RTO), i.e. the duration of time within which a business process or service must be restored in the event of a business continuity incident in order to avoid unacceptable consequences to the business associated with a break in continuity.
- **RPO**: The Recovery Point Objective (RPO), i.e. is the point in the past working backwards from a disaster, where data can be recovered in a usable format, usually through a backup, to ensure normal operation of impacted systems. This measure also assesses the potential data lost during an incident.

The Council's Technology Resilience Arrangements

The Corporate Resilience Team – is responsible for maintaining the Council's operational resilience framework. This includes ensuring that all Council services complete and regularly review business BIAs that assess the criticality of their services, and specify appropriate RTOs and RPOs for their recovery in the event of a resilience incident.

When completing BIAs Council services are required to provide details of the "level of operation they would have to reach in order to prevent the impact becoming unacceptable" as well as "when they would like to reach that level by".

Following review of BIAs by the Corporate Resilience Team, the relevant technology elements for systems managed by Digital Service and CGI (excluding and cloud based shadow IT systems that are managed directly by services) should then be provided to the Council's Digital Services Team for

discussion and review and potential inclusion in the Council's overarching technology resilience and disaster recovery plans managed by CGI.

Digital Services and CGI – Some Technology services are delivered through a partnership arrangement between the Council's Digital Services team and CGI who work together with services to identify and assess technology risks associated with the systems that they manage, and deliver appropriate resilience solutions within agreed contractual timeframes.

Digital Services management has confirmed that contractual recovery time and point objectives for systems recovery were agreed with Heads of Divisions prior to finalising the CGI contract, and that recovery requirements for the Council's Priority 1 systems can be altered via the established change management process.

The Council's contract with CGI confirms that where CGI provide services, they are responsible for:

- Disaster Recovery testing
- Client Service Reviews
- Availability and Capacity Management
- Continual Service Improvement

Relevant CGI Technology Resilience Contract Clauses

1) **Disaster Recovery and Supplier Business Continuity plans (Schedule 8.6 section 6)** - should be *"reviewed every 6 months, when major changes of scope apply, following a DR exercise, within 3 calendar months following a DR invocation, when requested as part of an audit and when required by the council".*
2) **Business Continuity and Disaster Recovery (Schedule 8.6 section 7)** - the Supplier (CGI) shall "*test services designated as Priority 1 within CGIs Contractual Obligations (OBS) Register on an annual basis*".
3) The current minimum CGI recovery time objective (RTO) service level for recovery of the Council's critical systems is 4 hours as detailed in the CGI and Council Service Continuity Plan. This SLA was agreed when the initial CGI contract was awarded in 2015.

Technology Resilience Governance Arrangements

Monthly Disaster Recovery Project Boards have been established to discuss progress with the Disaster Recovery testing schedule, and are attended by Digital Services and CGI, with details of meeting outcomes provided to the ICT-Resilience sub group.

The joint CGI and Digital Services technology resilience sub-group meets every two months to discuss technology resilience issues and risks to support service improvements. The Council's Resilience Group (chaired by the Corporate Resilience Team) receive the minutes of the sub-group meetings.

CGI also provides a monthly Client Services Report (CSR) to the Council's Digital Services Team that includes a summary of service level performance against a set of eight KPIs including Severe Incident Response and Resolution; Business Continuity; and Disaster Recovery. The report also includes a breakdown of availability and capacity metrics for all Priority 1 systems. The CSR report is shared with relevant stakeholders by e mail.

Covid-19 impacts

The Covid-19 pandemic had an immediate effect on the City of Edinburgh Council (the Council) by changing the way employees work, and citizens engage with the Council. To support this, the Council implemented some immediate technology changes including; increasing remote network access capacity from 3K to 5K users; implementing 'use your own device'; and implementation of MS Teams for employee engagement and collaboration. The Council's technology resilience will continue to be tested for the duration of the pandemic.

Recent Internal Audit Reviews

The Council's operational resilience was reviewed in September 2018 and 5 findings (2 High; 2 Medium; and 1 Low) were raised. The second High rated finding raised, highlighted that business impact assessments (BIAs) and service resilience plans were only partially complete across the Council, did not include specification of recovery time and point objectives for systems; and that no comparison had been performed between Council system recovery requirements and CGI contractual arrangements for the services that they provide.

Technology disaster recovery arrangements were last reviewed in May 2016, following the transition of managed technology services from BT to CGI in April 2016. One High rated finding was raised reflecting that the design of the Council's disaster recovery programme had been agreed, but no testing had yet been performed.

Scope

The objective of this audit was to:

- establish the effectiveness of the Council's technology risk assessment and resilience planning processes, and their application during Covid-19;
- determine CGI's ability to recover the Council's Learning and Teaching and Corporate networks and systems in order of criticality and in line with contractually agreed recovery time and recovery point specifications.

Limitations of Scope

The scope of our review was limited as follows:

- Technology incident and problem management and change management processes as these areas are covered by separate reviews included in the 2019/20 and 2020/21 Internal Audit annual plans.
- Resilience of individual technology applications; hardware; systems; or services, but the review did consider resilience in a wider context across the Council.

Reporting Date

Our audit work concluded on 11 February 2021 and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 4

Summary of findings raised	
High	Critical Systems Recovery Timeframes and Council Service Continuity Plans
Medium	Business Impact Assessments
Medium	Disaster Recovery Testing
Medium	Technology Resilience Governance Arrangements

Opinion

Our review identified a number of significant and moderate control weaknesses in the design and effectiveness of the Council's technology resilience control environment and governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed, and that the Council will be able to restore critical systems and services in line with agreed recovery time and point objectives in the event of a technology resilience incident.

Four findings (one High and three Medium) have been raised, reflecting the need to:

1. either align recovery timeframes for critical systems supporting Priority 1 services with the agreed CGI service levels or make alternative resilience arrangements for these systems, and update the Council's Technology Service Continuity Plan that is maintained by CGI covering the services that they provide (refer finding 1 below);
2. perform a review of all business impact assessments to ensure that all critical systems have been identified with appropriate recovery time and point objectives specified, and review this assessment following any significant resilience incidents (refer finding 2 below);
3. refresh disaster recovery test plans and recommence testing (refer finding 3 below); and
4. review and refresh technology resilience governance arrangements (refer finding 4 below).

The need to review system recovery time objectives and ensure that they were either aligned with agreed CGI service levels, or alternative resilience arrangements established was initially raised in the September 2018 Operational Resilience audit, with an original completion date of 31 July 2019.

Initial completion timeframes for open resilience assurance findings raised in the September 2018 audit have been extended by management to allow the Council to respond to Covid-19.

Following the refresh of BIA's by the Corporate Resilience team in January 2020, directorates and divisions are now working towards completing BIAs by May 2022. A Corporate Resilience exercise to review any gaps between recovery timeframes specified by the Council and the CGI four hour service level is also in progress for Priority 1 systems, with an expected completion date of December 2023.

The Corporate Resilience team submitted a list of Essential Activities highlighted through the BIA process to CLT in March 2019 for their consideration and sign off. The work to review BIAs, paused during the Covid-19 response, is due to commence in April 2021. This exercise will include the

identification of gaps in protocols and their development, with Directorates. A Council wide thematic Covid-19 lessons learned exercise is also scheduled to be performed by the Council's Resilience team.

Areas of good practice

The following areas of good practice have been identified:

1. **Technology Resilience Framework** - A framework has been embedded within the contractual obligations for delivery of technology services by CGI. Schedule 8.6 of the Supplier Agreement details the Business Continuity and Disaster Recovery requirements, which includes the necessary governance of plans and the conditions to invoke and exercise plans. An Operational Framework Document sits underneath the contractual obligations and describes CGI's key practices and activities for identifying and managing risks, and review of services and service improvement through the tracking and reporting of SLAs and KPIs.
2. **Disaster Recovery Testing** - Implementation plans for disaster recovery tests comprehensively capture the test approach, implementation plan, risks associated with the test, testing results and the pre and post test approvals. The plan also captures any post review issues and actions with owners, which are discussed during the monthly DR Project Board meetings.
3. **Skills and Experience** - Skills and Experiences is a general obligation within the contract that requires CGI to provide “appropriately qualified, trained and experienced employees, and to provide services with reasonable skill, care and diligence". The Operational Framework Document also includes details of the roles with both the Council and CGI that support delivery of CGI services, and the responsibilities associated with these roles.
4. **CGI's performance** - is assessed based on their delivery of services against the agreed Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) service levels, with monthly performance outcomes detailed in the Client Services Report.

3. Detailed findings

1. Critical Systems Recovery Timeframes and Council Service Continuity Plans	High

Directorates and Divisions

1. Review of the CGI contract; business impact assessments (BIAs) for 14 of the Council’s 32 Priority 1 Council services (refer details included at Appendix 4) and discussions with Service Managers and Heads of Divisions established that:

   a) Where Priority 1 services have identified shorter system recovery timeframes than the current four hour CGI service level, they must either accept the four hour CGI service level; request a contractual change through the established change process; or implement and rely on alternative resilience arrangements that potentially include manual operations. This approach is not aligned with good practice as RTOs should be driven by business needs. Digital Service management has advised that a four hour response is the current industry standard ‘best response’ timeframe.

b) All 14 Priority 1 services where BIAs were reviewed confirmed that they cannot align with the contractually agreed four hour CGI SLA as they require a two hour timeframe for recovery of their systems.

a) None of the 14 Priority 1 services have established alternative plans to ensure that systems can be recovered within two hours in the event of a resilience incident.

Digital Services and CGI

2. Review of the Council's Service Continuity Plan created and maintained by CGI that details the continuity and contingency arrangements for all CGI managed systems established that:

   a) It had not been reviewed and updated since12th December 2016. However, the supporting controls schedule includes review timeframes that are aligned with the requirements detailed in schedule 8.6, section six of the contract, which are:

      - every 6 months, when major changes of scope apply;
      - following a DR exercise;
      - within 3 calendar months following a DR invocation; and
      - when requested as part of an audit and when required by the council.

   b) CGI confirmed that they had reviewed the plan internally over the years but had not yet provided an updated version to the Council. However, no evidence of the internal reviews and review completion dates were provided by CGI

Risk

The potential risks associated with our findings are:

Directorates and Divisions

- Critical Council systems supporting services assessed as Priority 1 by Council divisions cannot be recovered within timeframes specified by the Council in the event of a technology resilience incident.
- Additional costs associated with agreeing alternative resilience arrangements with either CGI or alternative providers to ensure that critical systems can be recovered within two hours (where possible).
- Some services may be unable to revert to manual operations in the event of a significantly longer term resilience event.

Digital Services and CGI

- The Council's Service Continuity Plan that covers systems managed for the Council by CGI no longer meets the Council's requirements and cannot be effectively applied in the event of a resilience incident.

1.1 Recommendation: Corporate Resilience and Directorates - Critical Systems Recovery Timeframes

Open Internal Audit Findings

This high rated finding was initially raised in the Operational Resilience audit completed in September 2018 (finding 2). The audit recommendation was that recovery time and point objectives for CGI

hosted systems should either be aligned with established CGI contractual recovery arrangements, or change requests initiated where shorter recovery timeframes were required by Service Areas.

The management response confirmed that business impact assessment (BIA) templates would be reviewed by the Corporate Resilience Team, including recovery objectives, in conjunction with key stakeholders with an initial completion date of 31 July 2019.

Current Status

Initial completion timeframes for open resilience assurance findings raised in the September 2018 audit have been extended by management to allow the Council to respond to Covid-19.

Following the refresh of BIA templates and review of some BIAs by the Corporate Resilience team in January 2020 (this work was paused due to the impacts of Covid-19), there is an open action on all directorates to ensure that BIAs are completed using the refreshed templates by May 2022.

A Corporate Resilience exercise is also ongoing to review any gaps between recovery timeframes specified by the Council and the CGI four hour service level, with an expected completion date of December 2023.

Proposed Action for all Directorates

To avoid raising duplicate findings, the existing directorate actions due for completion by May 2022 will be updated to include the requirement for directorates to ensure that the 14 Priority 1 services system recovery times are either aligned with the existing CGI service levels; change requests initiated to request faster CGI recovery times; or alternative resilience arrangements established for these systems.

1.2 Recommendation: Council Service Continuity Plans

Digital Services and CGI management should:

1. Request that CGI perform a review of the Council's Service Continuity Plan to confirm that technology service continuity arrangements for systems supported by CGI remain appropriate
2. Digital Services will then review the refreshed Service Continuity Plan and provide feedback.
3. CGI will be requested to establish appropriate governance arrangements through either the Disaster Recovery Project Board or Technology Resilience sub-group to ensure that the service continuity plan is reviewed and refreshed in line with the requirements detailed in Schedule 8.6, section 6 of the CGI contract which are:
    - every 6 months, when major changes of scope apply;
    - following a DR exercise
    - within 3 calendar months following a DR invocation; and
    - when requested as part of an audit and when required by the council.

1.2 Agreed Management Action: Council Service Continuity Plans

This action will be implemented as recommended by Internal Audit.

1. The Council's Service Continuity Plan and Digital Services Contingency Plans will be reviewed and refreshed by CGI and finalised and agreed with Digital Services. It should be noted that additional costs will be incurred if recovery requirement timeframes of less than four hours is feasible, but is

outwith CGI's agreed contractual requirements. Where the cost is significant, risk acceptance may be required.

2. It is acknowledged that there have been no Disaster Recovery Project Board meetings since circa November 2019. CGI will re-establish the Disaster Recovery Project Board (or another appropriate equivalent governance forum), and this will be supported by a clearly defined terms of reference that confirms the Board's objectives ; responsibilities; and attendees.
3. The Council's refreshed Service Continuity Plan will then be refreshed in line with established contractual requirements, and at least every six months.
4. The Council's P1 BIAs will also be reviewed every six months as part of the same process.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director, Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Bell, Technical Architect; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial & Risk Lead; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and Assurance; Pete Scott Service Delivery Manager, CGI; Michael Fernandez Project Manager, CGI	**Implementation Date:** 16th December 2022

2. Business (System) Impact Assessments — Medium

Review of the current approach applied to support completion of Business Impact Assessments (BIAs) (and specifically systems impact assessments) across the Council and a sample of six Priority 1 BIAs (refer Appendix 4) confirmed that:

1) No overarching view of completed BIAs is performed to confirm that the Council's most critical systems have been identified and appropriate recovery time and recovery point objectives specified by Council services and divisions.
2) None of the six Priority 1 BIAs had been reviewed since February 2019, which is not aligned with the annual review requirements specified in the Council's resilience framework. Management confirmed that this was due to the impact of the COVID-19 pandemic on the Corporate Resilience Team.
3) Two of the Digital Services priority 1 BIAs for recovery of services provided by the Digital Services team (telephony and systems, and project delivery and change) generically referenced "All Key Core Council Applications" in relation to application dependencies across Council systems in both the body of the BIA and supporting appendices, with no reference to the specific systems.

Risk

The potential risks associated with these findings are that:

- Lack of consistent assessment of requirements for recovery of critical systems in Business Impact Assessments (BIAs).

- Recovery of critical systems may not be accurately prioritised following a technology resilience event.

2.1 Recommendation: Review Council Business Impact Assessments to Identify Critical Systems

Points 1 and 2 - the Digital Services and Corporate Resilience Teams should:

Digital Services

1. Produce guidance on the areas to be considered and how to assess / rate the criticality of systems as part of the business impact assessment process. This guidance will include details of the current recovery time and point objectives that have been contractually agreed with CGI, and recommend that alternative arrangements (including consideration of manual processes) should be established where these timeframes are not sufficient to meet service needs
2. Publish the guidance on the Council's intranet (the Orb) and in Manager's News.
3. Update the content of the user access management framework to reinforce the importance of ensuring that systems criticality (including recovery time and recovery point objectives) has been considered and included in business impact assessments and is reassessed at an appropriate frequency.
4. The refreshed user access management framework will also be published on the Orb and included in Manager's News.

Corporate Resilience

5. Perform a review of all business impact assessments (BIAs) and confirm that all services have assessed systems criticality (in line with Digital Services guidance) as part of their BIAs, and have established alternative arrangements where agreed CGI systems recovery service levels are not aligned with service requirements.
6. Provide feedback and challenge where systems impact assessments have not been completed; are not completed in line with the guidance; or where alternative resilience arrangements have not been established.
7. Prepare a consolidated list of all system impact assessments and share this with Digital Services for subsequent provision to CGI and inclusion in technology resilience plans.
8. Review this assessment following major incidents that impact normal operations (e.g. an external event or crisis like the COVID-19 pandemic) as part of lessons learned to determine whether system criticality should be reassessed.
9. Request services to reassess system criticality where required and provide the consolidated outcomes to Digital Services and CGI (where services are provided by CGI and recovery timeframes are within the contractually agreed timeframe) for inclusion in technology resilience plans, or consider alternative solution in line with Digital Services guidance.

2.1a Agreed Management Action: Digital Services - Business Impact Assessment Guidance

Digital Services Management will:

1. Produce guidance on the areas to be considered and how to assess / rate the criticality of systems as part of the business impact assessment process. This guidance will include details of the current recovery time and point objectives that have been contractually agreed with CGI, and

recommend that alternative arrangements (including consideration of manual processes) should be established where these timeframes are not sufficient to meet service needs

2. Publish the guidance on the Council's intranet (the Orb) and in Manager's News.
3. Update the content of the user access management framework to reinforce the importance of ensuring that systems criticality (including recovery time and recovery point objectives) has been considered and included in business impact assessments and is reassessed at an appropriate frequency.
4. The refreshed user access management framework will also be published on the Orb and included in Manager's News.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nicola Harvey, Head of Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Bell, Technical Architect; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial Team Lead; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and Assurance	**Implementation Date:** 31 March 2022

2.1b Agreed Management Action: Corporate Resilience – Supporting Directorates with Completion of Business Impact Assessments

To support Directorates with completion of BIAs by 31 December 2022 (note that this is an open IA finding raised in the September 2018 Operational Resilience audit) and address points 5 and 6 in the finding, Corporate Resilience Management will:

1. Liaise with Resilience Management Information System (MIS) supplier to determine how to incorporate required information on systems into MIS, in consultation with the Council Resilience Group; and
2. Incorporate checks and challenge into the BIA process and communicate to Directorates

Owner: Stephen Moir, Executive Director of Corporate Services **Contributors:** Nick Smith, Service Director, Legal and Assurance; Gavin King, Head of Democracy, Governance & Resilience; Mary-Ellen Lang, Corporate Resilience Manager; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and Assurance	**Implementation Date:** 30 September 2021

2.1c Agreed Management Action: Corporate Resilience – Sharing Systems Information with CGI and Digital Services

During the refresh of Directorate Business Impact Assessments and to address point 7 in the finding, Corporate Resilience Management will:

1. Provide quarterly updates on systems identified during the BIA process, once commenced; to be confirmed as received and shared with / implemented by CGI (also on a quarterly basis) by Digital Services.

Owner: Stephen Moir, Executive Director of Corporate Services	**Implementation Date:** 31 December 2022

Contributors: Nick Smith, Service Director, Legal and Assurance; Gavin King, Head of Democracy, Governance & Resilience; Mary-Ellen Lang, Corporate Resilience Manager; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and Assurance	

2.1d Agreed Management Action: Corporate Resilience – Refresh BIAs following Resilience Exercises or Major Incidents

Following completion of resilience exercises or after major incidents, and to address points 8 and 9 in the finding, the Corporate Resilience team will:

1. include impact on system criticality as part of corporate debrief process and cascade to Directorates. Directorates to share any impacts identified during debriefs to Digital, copying in Resilience.
2. Request services to reassess system criticality where required and provide the consolidated outcomes to Digital Services and CGI (where services are provided by CGI and recovery timeframes are within the contractually agreed timeframe) for inclusion in technology resilience plans.

Owner: Stephen Moir, Executive Director of Corporate Services **Contributors:** Nick Smith, Service Director, Legal and Assurance; Gavin King, Head of Democracy, Governance & Resilience; Mary-Ellen Lang, Corporate Resilience Manager; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and Assurance	**Implementation Date:** 31 December 2021

2.2 Recommendation: Review of Digital Services Business Impact Assessments

Point 3 - Digital Services should:

Review and refresh Digital Services Business Impact Assessments (BIAs) for the telephony and systems and project delivery and change services that they provide across the Council and ensure that details of specific applications are included in relation to application dependencies across Council systems as part of the review of BIAs scheduled for completion in April 2021.

2.2 Agreed Management Action

The Digital Services Business Impact Assessments (BIAs) will be reviewed and refreshed for the telephony and systems and project delivery and change services that they provide across the Council, and will be updated to include details of specific applications in relation to application dependencies across Council systems.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director, Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Bell, Technical Architect; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial & Risk Lead; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and	**Implementation Date:** 30 June 2022

Assurance; Pete Scott Service Delivery Manager, CGI; Michael Fernandez Project Manager, CGI	

3. Disaster Recovery Testing — Medium

Review of disaster recovery testing arrangements and Disaster Recovery Project Board meeting minutes confirmed that:

1) The December 2019 Disaster Recovery Project Board minutes included reference to the contractual obligation to test all Priority 1 systems within two years, which is not consistent with the annual testing requirements specified in the contract at Schedule 8.6 section 7.

2) Review of the CGI Disaster Recovery schedule for January 2018 to January 2020 confirmed that 23 of the Council's 24 priority 1 systems (refer Appendix 4) were not tested annually in line with contractual requirements, with only the SWIFT system tested. The plan did include seven mixed scenario based and specific technology system tests that were performed based on previous major incidents (for example database and data centre fail overs), however these included mostly Priority 2 and third party systems.

   Management has confirmed that this is attributable to focus on testing new technologies that were being implemented.

3) No schedule has been created detailing planned disaster recovery tests from January 2020 onwards.

   CGI management advised that tests have not been planned or completed due to the pandemic, as this could cause unnecessary disruption to services operating in the ongoing Covid-19 resilience environment.

   Digital Services management confirmed there had been no meetings to discuss planned disaster recovery tests since November 2019.

Risk

The potential risks associated with our findings are that:

- The Council is currently unable to confirm that the full population of critical systems supporting delivery of Priority 1 services can be recovered in the event of a technology resilience incident, impacting service delivery.

3.1 Recommendation: Disaster Recovery Testing

CGI and Digital Services management should:

1. prepare a disaster recovery testing schedule that includes (but is not limited to) annual disaster recovery testing of all Council CGI managed priority 1 systems;
2. share the disaster recovery testing schedule with the Council's Resilience Manager;
3. reinstate ongoing disaster recovery testing as soon as possible, recognising the ongoing challenges associated with the current Covid-19 operating environment;

4. implement appropriate Disaster Recovery Project Board monitoring arrangements to ensure that all priority 1 systems are tested annually in line with agreed contractual requirements, with the rationale documented in meeting minutes where the schedule of testing cannot be completed, or a decision is taken not to test specific systems.

3.1 Agreed Management Action: Disaster Recovery Testing

Both Digital Services and CGI management has advised that there was a verbal agreement to reduce the frequency of disaster recovery testing and adopt an alternative approach with focus on specific systems as completion of testing in line with contractual requirements was a significant undertaking that could potentially result in frequent system outages.

It is acknowledged that this agreement was not documented.

1. the disaster recovery testing approach and schedule will be reviewed and agreed with CGI and formalised through the governance process. This will include consideration of all of the Council's priority 1 systems;
2. The rationale for any priority 1 systems that are not included (at least annually) in the disaster recovery testing schedule will be recorded, and the relevant directorates and divisions who use these systems advised;
3. once the DR testing approach has been agreed, testing will be performed with completion and outcomes monitored through relevant governance forums and
4. the disaster recovery testing schedule and testing outcomes will be shared with the Council's Resilience Manager.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director, Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Bell, Technical Architect; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial & Risk Lead; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and Assurance; Pete Scott Service Delivery Manager, CGI; Michael Fernandez Project Manager, CGI	**Implementation Date:** 16 December 2022

4. Technology Resilience Governance Arrangements — Medium

1. Review of the Council's established technology resilience governance arrangements confirmed that:
   a) Disaster Recovery Project Board meetings are attended by Digital Services and CGI, with outcomes and updates provided to the ICT-Resilience sub-group.
   b) The Corporate Resilience Team receives updates on the Council's technology resilience arrangements through receipt of minutes of the two (bi) monthly Digital Services and CGI ICT Resilience sub-group meetings.

2. Review of arrangements supporting the operation of the two monthly ICT Resilience Sub-group confirmed that:

   a) CGI representation is not mandated at the ICT-Resilience sub-group although they are invited to all meetings.

      Review of a sample of three ICT Resilience sub-group meeting minutes (September - December 2020) highlighted that updates in relation to disaster recovery requested by the Council in September were not addressed until a CGI representative attended the December meeting, where responses were provided, and an action plan determined.

   b) Whilst disaster recovery is included as a standing agenda item on the ICT-Resilience sub-group, review of meeting minutes confirmed that disaster recovery updates were requested in two instances (September and December 2020) and were not provided.

   c) The monthly CGI Client Services Report that includes a summary of performance against key performance indicators (KPIs) (including technology resilience and disaster recovery KPIs) and availability and capacity metrics for Priority 1 systems is not provided to the ICT resilience sub-group.

Risk

The potential risks associated with our findings are:

- Risks associated with technology resilience testing performed by CGI are not identified; recorded; assessed; and managed.
- CGI technology resilience performance issues are not identified and addressed.
- Technology resilience risks and are not reflected in the Council's corporate resilience plans.

4.1 Recommendation: Technology Resilience Governance Arrangements

CGI and Digital Services management should:

1. Engage with the Corporate Resilience Team to determine the best approach to ensure that they are aware of planned disaster recovery tests and also receive comprehensive details of completed test outcomes and actions to be implemented (by both Digital Services / CGI and directorates / divisions) to address any issues identified once disaster recovery testing has been completed.
2. For the ICT-Resilience sub-group:
   a) establish quorum arrangements (that include CGI representation) or, where this is not possible, establish a process to ensure that all questions raised at meetings are communicated to CGI following the meeting with a request for responses to be provided;
   b) ensure that disaster recovery updates are consistently provided in line with standing agenda item requirements, with outcomes and actions from discussions recorded and monitored through to implementation;
   c) provide a copy of the monthly CGI Client Services Report to the group to support their discussions on disaster recovery.

4.1 Agreed Management Action: Technology Resilience Governance Arrangements

1. The ICT-Resilience sub-group does feed into the Council's Resilience. This includes providing an update on disaster recovery testing, but only when there is a progress update to be provided.

   It is acknowledged that there have been no recent updates provided due to the limited disaster recovery testing performed as highlighted in finding 3.

2. The ICT Resilience sub-group is an operational meeting that covers Disaster Recovery Project Board outcomes within its scope and feeds into the Council resilience group. CGI and Digital Services governance arrangements are currently being discussed, and the ICT-Resilience sub-group will be included in these conversations. As additional governance requirements could result in additional costs, the discussions will focus on whether CGI attendance at this meeting is covered by existing contractual obligations. Where this is not the case, the ICT-Resilience sub-group will continue to operate on the basis of a goodwill commitment from CGI to attend.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director, Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Bell, Technical Architect; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial & Risk Lead; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant, Legal and Assurance; Pete Scott Service Delivery Manager, CGI; Michael Fernandez Project Manager, CGI	**Implementation Date:** 30 June 2022

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation of the organisation which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation of the organisation.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the organisation.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Please see the Internal Audit Charter for full details of opinion ratings and classifications.

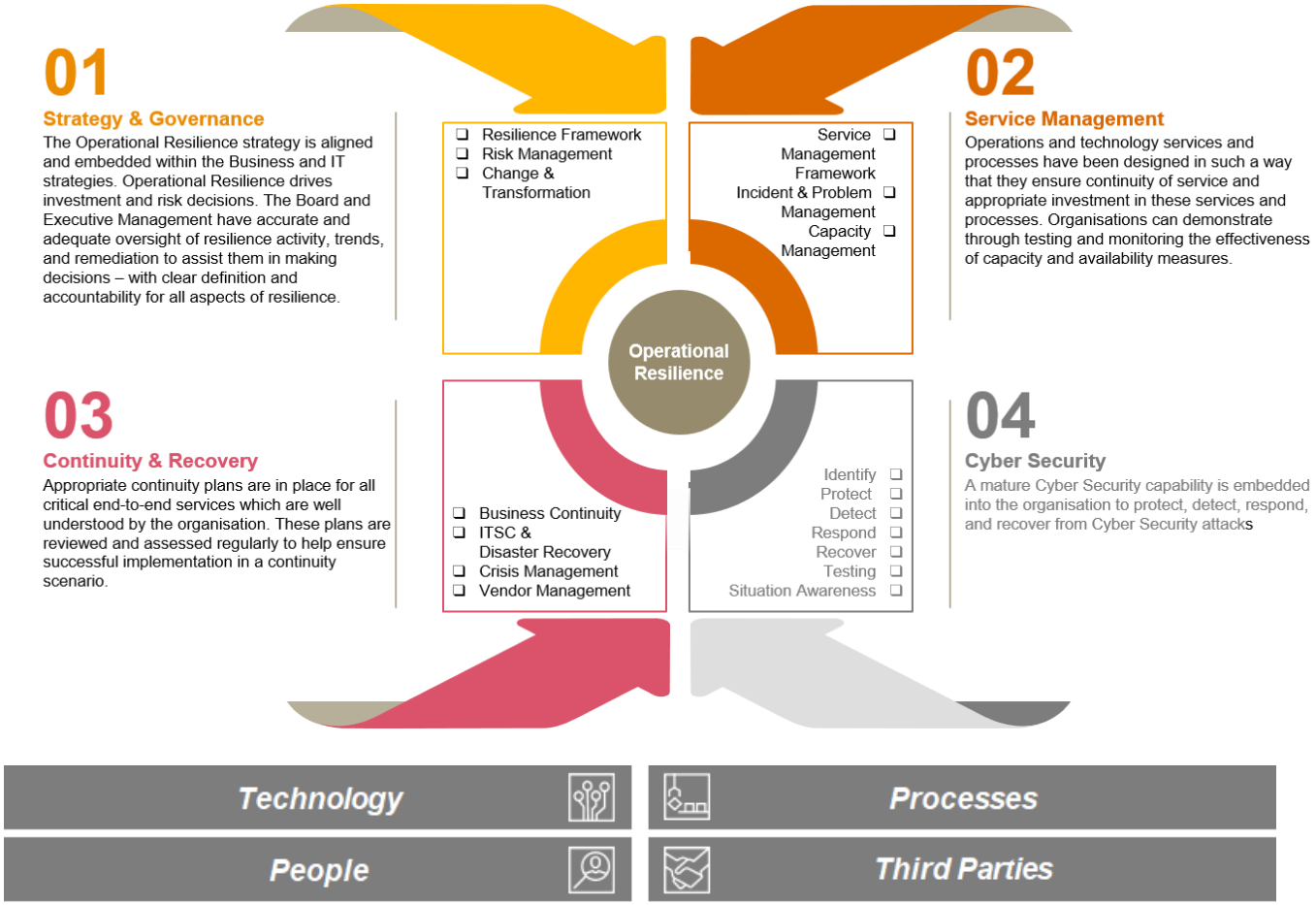
Appendix 2: Areas of audit focus

The areas of audit focus and related control objectives included in the review were:

Audit Area	Control Objectives
Critical systems	• An exercise has been performed to map critical business services to the systems that underpin their operations and where relevant the third parties that support them. • An exercise to identify single points of failure in critical networks and systems has been performed, with actions taken to address and remediate these where possible.
Resilience plan	• The existing resilience framework and plans have been understood and agreed between the Council and CGI. • Resilience plans are updated in a timely manner to reflect changes detailed in change requests for example implementation of new technology systems, or changes in criticality assessments for existing systems. • Triggers for initiation of resilience plans (for example initiation of the Covid-19 resilience response) have been defined and clearly communicated and include a range of documented crisis scenarios with guidelines on the initial steps to be followed by front line support staff. • Alerts are configured to notify key stakeholders when a crisis or disaster occurs. • Recovery details exist with specific instructions for returning systems to a working state within defined timescales and with minimal data loss.
Testing	• A test programme and schedule exist which covers the full scope of critical networks and systems. • Resilience testing is performed on a regular basis. This testing includes a combination of actual testing (e.g. systems are shut down and restored) and scenario-based testing
Resilience Reporting & Lessons Learnt	• A report is produced at regular intervals to provide senior stakeholders with metrics on resilience and disaster prevention measures. • Where applicable, resilience plans have been updated to reflect lessons learnt from COVID-19. • A risk assessment has been done to consider new resilience risks from the lessons learnt from COVID-19 and to identify actions to mitigate such risks.
Continuous Improvement	• Results arising from resilience plan testing or incidents are documented, including lessons learned. These results are used to improve resilience plans and to continuously enhance the service provided.
Skills and Experience	• The requirement for CGI to provide suitably skilled and experienced resources to support the resilience service is clearly specified in the contract.

Appendix 3: Operational Resilience Framework

Below is PwC's Operational Resilience Maturity Assessment framework 'Lite Version' (ORMA Lite). It has been tailored for non-financial services organisations, and is grounded in the key expectations to manage critical technologies, people, processes and third parties. It highlights the importance of technology in the operational resilience ecosystem.



Appendix 4: Details Supporting Testing Outcomes

Priority 1 Council services where system recovery times are not aligned with current CGI Service Levels:

1. Additional Support for Learning & Special Schools
2. Children's Social Work Practice Teams and Review Service
3. Secondary Schools
4. Primary Schools
5. Infrastructure
6. Road Services
7. Customer Contact
8. Customer Contact & Transactions
9. Customer Services
10. Finance
11. Cultural Venues
12. Looked After Children
13. PILOT
14. Scientific Services, Bereavement and Registration

Priority 1 business impact assessments not reviewed since February 2019:

1. Customer Hub - Location Plan
2. Customer Hub - Service Area Plan
3. Criminal Justice - Management of criminal justice group work services
4. Schools - Delivery of Learning and Teaching in Secondary Schools
5. Digital Services - Service Management (telephony and systems)
6. Digital Services - Project Delivery and Change

Priority 1 systems that have not been tested annually:

1. PPSL Debt Management System
2. Oracle eFinance / EBusiness
3. iTrent Payroll
4. iWorld Revs and Bens
5. AIM / ACR
6. Contact Centre MiCC
7. iWorld Housing
8. Confirm
9. Batch Printing
10. EDM Workflow 360
11. Cognos
12. Citizen Digital Enablement (CDE)
13. Homeless Care Information Database
14. IDOX / Uniform
15. CAFM
16. Oracle eFinance Discoverer

17. webCAPTURE & eCAPTURE (GovTech)
18. eFinance WRM
19. WebRoster
20. JADU (Internet)
21. JADU (Intranet)
22. AI.SYNCPOINT / SharePoint
23. Total Repairs

The City of Edinburgh Council

Internal Audit

Network Management (Corporate and Learning and Teaching Networks)

Final Report

2nd August 2021

RES2003

Overall report rating:

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.

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2020/21 internal audit plan approved by the Governance, Risk and Best Value Committee in September 2020. 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 a number of 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.

1. Background and Scope

Background

Network management is the process of administering, managing, and operating a data network. Typically, the network is managed using software and hardware applications to collect and analyse data, and push out configuration changes for improving performance, reliability and security.

Effective management of the network validates that the organisation's data, assets and information are stored securely, and the information flowing through it is secure from both internal and external attacks. The effectiveness relies on the principle of defence in depth where layers of security components provide the necessary protection from inappropriate or unauthorised access to the network. This process includes, but is not limited to:

- A robust security policy built on good practices, using recognised standards;
- Access management controls addressed by identity management;
- External perimeter control using firewalls to protect the internal network from external intrusion;
- Virtual private networks (VPNs) to allow authorised traffic through the firewall, using encryption techniques to prevent eavesdropping, and physical devices (tokens) of which the user must have custody to further enhance authentication;
- Risk management to evaluate and identify networks and resources requiring enhanced security; and
- Internal network segmentation, limiting access of data in certain locations to authorized users and restricting that area from others within the enterprise.

Network Management across the Council

The City of Edinburgh Council (the Council) operates two main networks, namely the Corporate network and the Learning & Teaching (L&T) networks. The corporate network is used by the majority of Council divisions, whilst the Learning & Teaching network is a digital learning environment for schools within the jurisdiction of the Council.

Both 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, and are subject to ongoing vulnerability scanning.

Network Security Accreditations

Following achievement of basic Scottish Government (SG) Cyber Essentials accreditation in June 2020, the Council has now obtained SG Cyber Essentials Plus accreditation in line with SG Cyber Resilience Public Sector Action Plan requirements. However, the Learning and Teaching network has not yet undergone any cyber essentials accreditation.

The Council is also required to maintain ongoing compliance with the UK Government's Public Services Network (PSN) requirements for the Corporate network. PSN is the UK government's high-performance network that enables public sector organisations to share resources. It unifies the provision of network infrastructure across the UK public sector into an interconnected "network of networks" to increase efficiency and reduce overall public expenditure. The PSN is part of the UK Government Digital Service and is managed by the Cabinet Office.

All PSN users are required to hold a valid PSN connection compliance (CoCo) certificate that ensures that all networks connected to the PSN meet basic UK Government security requirements.

The Council's current PSN certificate of compliance was awarded in March 2021 and remains valid until March 2022.

Both Cyber Essentials Plus and PSN accreditation involve completion of a 'point in time' independent review / health-check assessment to confirm the effectiveness of network security controls.

Previous Internal Audit Reports

The effectiveness of established CGI Partnership Management and Governance processes applied by the Digital Services team was reviewed in an Audit completed in July 2020. One medium rated finding was raised which highlighted (amongst other things) that:

1. Only one key performance indicator (KPI) is included in the CGI contract in relation to the security services that they provide for the Council, with some security related operational performance measures included in the monthly security operations report provided to the security working group.
2. The CGI contract does not include a specific requirement for provision of ongoing independent assurance from CGI to the Council in relation to the operational controls supporting the security and compliance aspects of CGI services. Instead, reliance is currently placed on the independent security reviews completed to support cyber essentials and cyber essential plus accreditations, in line with the Scottish Government cyber resilience framework requirements. However, cyber essentials and cyber essentials plus accreditation has not yet been assessed for the Council's Learning and Teaching network.

Management has recently advised that

1. The risks in relation to the limited security KPIs will be accepted on the basis that changes to contractual KPIs were not possible under the terms of the CGI contract, with ongoing performance monitored through established performance management and governance processes.
2. CGI provide copies of their external accreditations to the Council (for example ISO27001).

Scope

The objective of this review was to assess the adequacy of design of the key network security controls established to ensure effective management of both the Council's Corporate and Learning and Teaching networks.

Limitations of Scope

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

- The operating effectiveness of the controls was not assessed, and no sample testing was performed as part of this review.
- Review and testing of the configuration of network security controls such as firewalls, switches and router configurations was not performed.
- No network scans or security testing was performed on the network
- Voice and mobile communications were exempt from the review.
- Network security controls not operated by CGI and those in place in cloud environments or controls managed by other third parties were exempt from the review.

- Any aspect not specifically included in the detailed scope at appendix 2 were excluded from the scope of the review.

Reporting Date

Our audit work concluded on 12 April 2021 and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 4

**Summary of findings raised	
High	Network management documentation
High	Network management effectiveness and assurance
Medium	Network threat identification and risk assessment
Medium	Technical configuration of networks and network devices

** Findings relate to both Corporate and L&T networks. Refer to section 3 for details

Opinion

Our review identified some significant and moderate control weaknesses in the design and effectiveness of the control environment and governance and risk management frameworks established to support the secure management of the Council's corporate and learning and teaching networks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives of secure and effective management of the corporate and learning and teaching networks will be achieved.

The CGI Partnership Management and Governance Audit completed in July 2020 highlighted that the established CGI contract includes only one security key performance indicator (KPI), and does not include a specific requirement for provision of ongoing independent assurance from CGI to the Council in relation to the operational controls supporting the security and compliance aspects of CGI services.

Management has advised that the risks associated with limited security KPIs will be accepted on the basis that changes to contractual KPIs are not possible under the terms of the CGI contract, with ongoing performance monitored through established performance management and governance processes.

Management has also confirmed that reliance is currently placed on the independent security reviews completed to support PSN and cyber essentials and cyber essential plus accreditations, and external accreditations achieved by the Council. However, cyber essentials and cyber essentials plus accreditations do not currently include the Council's Learning and Teaching network; are performed annually; and both the independent security reviews and accreditations will vary in both scope and depth.

Additionally, our review has identified a number of areas where network management controls required to be significantly improved, that are not specifically covered by the generic security requirements and KPI included in the CGI contract, and have not been previously identified by the independent security reviews completed to support achievement of cyber essentials and cyber essentials plus accreditations.

Consequently, four findings (two high and two medium) have been raised highlighting the need to implement and enhance standard network security measures that would typically be performed as part of ongoing network management activities across both the corporate and L&T networks.

Further detail is included at section 3 below.

Areas of good practice

The following areas of good practice have been identified:

1. **Security reporting -** CGI prepares monthly reports for the Security Working Group that include some security metrics, for example, the number of vulnerabilities identified across the devices connected to both the Corporate and L&T networks; the number of devices patched and not patched; the number of security incidents experienced; threats detected across the network; and new and emerging threat intelligence. Management has advised that these are defined and provided in line with CGI's contractual requirements.
2. **Incident management** - An incident management process has been established, with CGI providing a Service Desk support to the Council where security and other incidents can be raised and escalated for resolution.
3. **Network access segregation for management** - Access to the network devices is limited to only CGI support staff through a defined Terminal Access Controller Access Control System (TACACS) that determines whether access is permitted to specific systems. This alleviates the risk of a non-CGI employee gaining access to the network devices and the possibility of malicious or inadvertent configuration changes.
4. **Network resilience considerations** - As part of the network architecture, CGI has considered and implemented resilient clusters of network devices and data centres to provide availability in a resilience event as agreed in the contract.
5. **Network threat monitoring** - threats to the network and network devices are proactively monitored by the Security Operations Centre (SOC) team. The SOC's threat intelligence feeds into CGI's management of the Council's network, with remediation activities based on the significance of risk posed to the Council. Threats identified by the SOC team are correlated with the latest vulnerability scan reports and risk assessed.
6. **Segregated security controls** - CGI maintains the same network security controls over both the Council's Corporate and L&T networks, with appropriate segregation both within the networks and from other networks. Network perimeter controls also include distributed denial of service (DDoS) protection on external firewalls, and restriction of movement between the Corporate and L&T environments.

3. Detailed findings

1. Network management documentation	High

We identified the following areas where network management documentation and information sharing in relation to both the Corporate and L&T networks requires improvement:

1. Review of the documentation produced and maintained by CGI to support ongoing management of the networks established that existing documentation does not describe all aspects of the networks and their security arrangements. Specifically:
   a) There is no evidence of a documented standard having been agreed between the Council and CGI that details how hardware or devices (for example network firewalls and routers) should be configured to connect to the networks; which services and devices are permitted to connect; and those that are blocked. Instead, a generic good practice configuration document is used by CGI to support configuration of Council network devices together with a low level design that defines how the network is configured in practice.
   b) Details of historic configuration changes for individual devices are not held in a centrally. Whilst it is possible to identify historic configuration changes through change requests and IT service tickets, this would take some time and is not efficient;
   c) There is high dependency on backups when rebuilding or re-imaging network devices to mirror the latest configuration.
   d) There is no documentation outlining defined fail-safe (mechanisms designed to ensure safe failure of devices with limited impact on other devices) and fail-over (transfer to a duplicate system) mechanisms to ensure that recovery is possible and key devices (for example firewalls, servers, and routers) remain available.
   e) There is no documentation that outlines the different ways that the Council's networks would recover from a potential failure (failure modes).
2. We also noted the following areas where engagement and information sharing between CGI and the Council in relation to network management and security could be improved:
   a) The Council had requested specific assurance from CGI on the effectiveness of network security controls on a number of occasions, and a clear response was not consistently provided. This situation was addressed, but required escalation resulting in delayed receipt of the information.
   b) Whilst security concerns are reported within multiple governance forums, the key Digital Services key point of contact for security matters is the Digital Services Security Manager who is responsible for oversight of the network security activities performed by CGI and challenging their performance and delivery. It is acknowledged that the Chief Digital Officer and other members of the management team also attend these governance forums.

Potential Risks Associated with Findings Raised

The potential risks associated with our findings are:

- Network devices could be incorrectly or inconsistently configured across Council networks increasing the risk of malicious intrusion.
- Networks cannot continue to operate or cannot be recovered in the event of an incident.
- The Council does not receive timely assurance from CGI in relation to network management and security control concerns raised.
- Security concerns are not communicated and addressed promptly in the absence of the Digital Services Security manager.

1.1 Recommendation: Network management documentation

1. Discussion should be held between Digital Services and CGI to confirm whether the current low level design applied by CGI meets the expected standard for the Council. The finally agreed standard should be documented and centrally maintained by CGI. This documentation should also include (but should not be limited to) details of services and devices that are permitted to connect; those that are blocked; and details of historic configuration changes for individual devices.
2. Where adjustments to the configuration images for the Council network devices are required, these should be implemented.
3. Details of network fail-safe and fail-over mechanisms and failure modes should be documented; maintained; and tested at an appropriate frequency by CGI.

1.1 Agreed Management Action: Network management documentation

1. Digital Services will risk accept this recommendation.
2. Digital Services will risk accept this recommendation.
3. Digital Services will review the current network DR processes, associated documentation and testing regime and agree an improvement plan if required.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director: Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Brown, Cyber Security Manager; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial Team Lead; Mike Bell, Digital Services Technical Architect.	**Implementation Date:** 31st March 2023

1.2 Recommendation: Engagement and information sharing

1. A clear process should be established to ensure that all requests from the Council for additional assurance or clarification in relation to the effectiveness of network security controls should be agreed with CGI and consistently applied.
2. Alternative arrangements should be established to ensure that security issues are communicated by CGI to the Council when the Council's Cyber Security Manager is absent from work.

1.2 Agreed Management Action: Engagement and information sharing

1. Digital Services Management will agree a process for the raising and monitoring of requests for additional assurance or clarification in relation to the effectiveness of network security controls incorporating an escalation path.
2. Alternative arrangements are already in place when the Council's Digital Services Cyber Security Manager is absent from work. Another officer has been assigned to work with the Cyber Security Manager and both he and the Chief Digital Officer have access to the necessary forums and communication paths by which security issues and incidents are raised,

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director: Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Brown, Cyber Security Manager; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial Team Lead.	**Implementation Date:** 31st March 2022

2. Network management effectiveness and assurance — High

Whilst it is acknowledged that management:

- has accepted the risks highlighted in previous audit reports in relation to limited security Key Performance Indicators (KPIs) included in the CGI contract;
- is placing reliance on completion of independent security reviews completed to support cyber essentials and cyber essential plus and PSN accreditations to confirm the effectiveness of CGI performance; and
- will receive copies of external CGI accreditations (for example ISO27001),

It should be noted that the independent security reviews and accreditations will vary in both scope and depth. For example, as ISO27001 permits organisations to select their accreditation topics, accreditation outcomes may not specifically cover network security. Additionally, ISO accreditation focuses mainly on established organisational standards and policies with limited controls testing.

We have identified the following areas where network management activities across both the corporate and L&T networks require improvement, and are unlikely to be covered by the independent reviews and accreditations noted above.

1. There has been no independent review of the effectiveness of, or independent assurance in relation to the following standard network management controls:
    a) The completeness and accuracy of network logging and monitoring processes to enable review of network activity from both within and outside the Council;
    b) Overall network configuration including defence in depth (multiple layers security controls within networks), separation and segregation of the network components to improve security;
    c) Completion of periodic tests of network failure modes, and confirmation of the effectiveness and speed of migrating to the secondary (fail-over) networks; and
    d) Adequacy of current network device configurations to confirm that they are aligned with industry / vendor standards recommendations.

2. Penetration testing is performed annually for the corporate network as part of the PSN accreditation process, and will also be an annual requirement as part of the Cyber Resilient Scotland: Strategic Framework. However, this testing currently has a limited scope, and does not include the L&T network.
3. The adequacy of the frequency of the weekly vulnerability scans has not been assessed and the risk associated with vulnerabilities identified have not been analysed.
4. The Council does not ensure assurance activities (for example outcomes of network configuration and access reviews) are carried out over all aspects of the network by reviewing documents produced by CGI or requesting additional evidence of assurance.

Risk

The potential risks associated with these findings are that:

- Network security threats and weaknesses are not identified and addressed;
- Cyber attacks are not effectively prevented;
- Additional L&T network risks are not identified as penetration testing has not been established.
- Networks cannot continue to operate or cannot be recovered in the event of an incident;
- The Council is unable to confirm whether CGI has met their contractual network management and security obligations.

2.1 Recommendation: Network management effectiveness and assurance

1. The Council should define a schedule of assurance activities reflecting network security, including around configuration, logging and monitoring of network devices, defence in depth and failure modes. The Council should also determine the level of documentation and metrics required to measure and track the assurance activities over the network and security management by CGI.
2. The Council should request periodic penetration tests over the Corporate and L&T networks. The frequency and scope of these penetration tests should be agreed based on the risks and threats faced by the Council.
3. The frequency and scope of the vulnerability tests should be reviewed, and the reports should be verified to ensure recurrence of vulnerabilities is minimal and all critical and high priority vulnerabilities are addressed within agreed timeframes.
4. Periodic tests on resiliency of the critical parts of the network and network components should be mandated by the Council. Where appropriate, independent assessment of the failure modes and effectiveness of resiliency should be performed. CGI should provide evidence of testing failure modes for both the L&T and Corporate network.

2.1 Agreed Management Action: Network management effectiveness and assurance

1. This action would primarily require contractual changes and will be risk accepted.
2. Digital Services professional opinion is that the annual and separate tests for PSN and Cyber Essentials plus coupled for the Corporate network with additional testing for new systems or devices on the network provides an acceptable testing regime. Digital Services have also requested that CGI penetration test the L&T network.

3. Digital Services professional opinion is that the existing vulnerability scanning frequency for both Corporate and L&T networks is acceptable and notes that this will also be coupled with Quarterly Assurance for the Corporate Network from CGI in the summer of 2021 which will cover information on vulnerability management over a period of time. Vulnerability scanning is carried out for all vulnerabilities on the network at the same time. Consequently, tracking a single vulnerability may not be possible and any evidence required to track a single vulnerability may need to be risk accepted.
4. Digital Services will review the current network DR processes, associated documentation and testing regime and agree an improvement plan if required.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director: Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Brown, Digital Services Cyber Security Manager; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial Team Lead; Mike Bell, Digital Services Technical Architect.	**Implementation Date:** 31st March 2023

3. Network threat identification and risk assessment — Medium

We identified the following areas where threat identification and risk assessment processes across both the corporate and L&T networks require improvement:

1. No security reviews are performed to confirm whether threats that are not linked to vulnerabilities previously identified from ongoing vulnerability scanning pose any additional risks to the Council;
2. No evidence is available to confirm that network risk assessments are consistently performed across the network in relation to planned security changes; and
3. There is no clear agreement between the Council and CGI that confirms when network risk assessments should be performed and how these should be documented.

Risks

The potential risks associated with our findings are that:

- Council networks may not be appropriately protected against new and emerging security threats; and
- Planned network security changes and decisions do not fully consider all potential risks.

3.1 Recommendation: Network threat identification

1. CGI should be requested to provide details of new and emerging security threats that have not been identified from vulnerability scanning to Digital Services;
2. Digital Services should consider whether network security tests are required to confirm that the Council is appropriately protected against any significant security threats, and instruct CGI to perform these tests; and

3. The integration between threat assessment, risk assessment and security testing should be reinforced with appropriate reporting to CEC to determine risk and follow-up actions to address the residual risks and handle the residual threats.

3.1 Agreed Management Action: Network threat identification

1. Digital Services considers that this is already in place. Details of new and emerging threats are already on the SWG reports and reported to CISSG. Ad hoc and urgent threats are updated directly to the Digital Services Cyber Security Manager as and when required,
2. Digital Services professional opinion is that the annual and separate tests for PSN and Cyber Essentials plus for the Corporate network coupled with additional testing for new systems or devices on the network provides an acceptable testing regime. Similarly, separate penetration testing for the L&T network has been requested to mirror the testing of the Corporate network. Vulnerability scanning is already taking place across Corporate and L&T networks.
3. Reporting of these is already in place as part of SWG reports and the outputs from both CE+ and PSN health checks. The same process will be applied to outputs from the penetration test on the L&T network. Risks raised from these are already raised, mitigated or added to relevant risk registers.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director: Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Brown, Digital Services Cyber Security Manager; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial Team Lead.	**Implementation Date:** 31st March 2023

3.2 Recommendation: Network risk assessments

1. The Council and CGI should formalise criteria for performing network risk assessments and apply a risk-based approach that is aligned with the Council's approved risk appetite statement when considering decisions and changes that could potentially impact network security; and
2. All completed risk assessments should be documented, with risks identified and recorded in relevant risk registers.

3.2 Agreed Management Action: Network risk assessments

1. Digital Services perform penetration testing/network healthchecks for PSN and Cyber Essentials plus on the corporate network as well as ad hoc tests. The process is already in place to review the outputs from these and agree to remediate or risk accept. Remediation may be contractual or at the request of the Council via the Change Management process. Similarly, once the output from penetration testing of the L&T network is available, the same review, remediation and risk processes will occur.
2. All risk assessments are documented and those currently in place have a corresponding entry in the relevant risk register.

Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director: Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Brown, Digital Services Cyber Security Manager; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial Team Lead.	**Implementation Date:** 31st March 2023

4. Technical configuration networks and network devices — Medium

We identified the following areas where network and device configuration across both the corporate and L&T networks require improvement:

1. Authentication of network users is reliant on Active Directory password-based authentication, with digital certificate authentication currently limited to device authentication and virtual private network (VPN) based access. Digital certificates only verify that the device accessing the network was issued by CGI and do not authenticate or verify the identity of the user in possession of the device;
2. There was no evidence of alerts being triggered when a network device is identified that deviates from the standard device configuration. Note that finding 1 also highlights that standard device configurations have not yet been agreed between the Council and CGI. .

Risks

The potential risks associated with our findings are:

- Malicious users could use devices provided by CGI with no additional authentication to access networks where user credentials and passwords have been compromised
- Instances where network devices are operating with unacceptable / unauthorised configurations cannot be detected.
- Malicious intrusion or proliferation of malware on the Learning and Teaching network managed by Digital Services.

This finding has been assessed as medium as these risks are mitigated (to an extent) by use of CGI digital certificates which confirm that devices presented to the network are devices provided by CGI. Our review has also confirmed that it would be difficult to forge these digital certificates as they are generated through the CGI trust centre.

4.1 Recommendation: Technical configuration of network and network devices

1. The requirements to establish Network Access Control (NAC) across Corporate and L&T networks should be assessed by the Council and CGI. The Council should consider requesting CGI to implement certificate-based authentication across the network, not just limited to VPN based access.
2. Following implementation of recommendation 1.1. above, configure alerts for network devices to notify administrators of non-compliant configuration settings across both L&T and Corporate networks.

4.1 Agreed Management Action: Technical configuration of network and network devices	
1. Digital Services will direct CGI to implement certificate-based authentication across the network in accordance with Schedule 2.4 of the contract. 2. Digital Services will risk accept this recommendation.	
Owner: Stephen Moir, Executive Director of Corporate Services, and John Knill, Vice President CGI **Contributors:** Nicola Harvey, Service Director: Customer and Digital Services; Heather Robb Chief Digital Officer; Mike Brown, Digital Services Cyber Security Manager; Jackie Galloway, Digital Services Commercial Manager; Alison Roarty, Digital Services Commercial Team Lead.	**Implementation Date:** 31st December 2023

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation of the organisation which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation of the organisation.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the organisation.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Please see the Internal Audit Charter for full details of opinion ratings and classifications.

Appendix 2: Areas of audit focus

The areas of audit focus and related control objectives included in the review were:

Area of Focus	Sub Process	Objectives
Governance and management of networks	In-house management	• Responsibilities have been assigned within the Council to appropriately manage and monitor the network and management information from the network devices in collaboration with CGI. • The security team has access to CGI's network management system, which is used as a central repository to configure, update and push policies to the network devices. • The logs from the network devices are shared to the managed SIEM tool for correlation, monitoring, identification of threats and to alert malicious behaviour.
	Third-party management	• Members of staff within the Council have been assigned responsibility over the liaison with CGI to ensure: ○ assurance over the confidentiality, integrity and availability of the network; ○ adequate performance of the network devices, and ○ appropriate actions are taken in an event of an incident • CGI provide proportionate information about the risks posed by the network to the Council, including: ○ Threats and vulnerabilities; ○ Performance; ○ Change including category of change; and ○ Incidents.
Confidentiality and integrity aspects of network security	Network perimeter control	• Network devices at all ingress and egress points are implemented by CGI and validated by the Council to prevent and detect unauthorised connections. • Network perimeters controls are layered to provide defence in depth protection to the Council's high risk/critical assets. • Network diagrams and other security control architecture is well maintained by CGI and the Council has adequate visibility over the network controls and architecture. • Base images have been created and documented for all network devices detailing the risk-based rationale behind the open ports and allowed / blocked services. • Posture checks to validate compliance to the base builds are performed periodically. Network devices that do not operate on baseline security standards trigger an alert and are managed promptly.
	Network configuration	• The wired and wireless network are configured by CGI with identical security controls and restrictions to prevent unauthorised access and data loss. • Configuration of the network devices are aligned to industry good practice, formally documented by CGI with sufficient documented risk assessments for exclusions and exceptions. • Features such as VPN tunnelling, URL/spam filtering, denial of service protection and proxies, have been considered and have

Area of Focus	Sub Process	Objectives
		been securely configured by CGI. Assurance over these features are sought by the Council periodically. ● The configuration of the network and the network devices are kept up to date, regularly security tested (penetration test and vulnerability scans) and reviewed to ensure adequacy, appropriateness and adherence to regulatory requirements. ● Only authorised services and websites have been whitelisted for successful connections. Exceptions to the services and connections are analysed by risk, documented and approval is sought through a formal change management process to reduce the risk of data loss through unauthorised data transfer.
	Network access and registration	● Policies and procedures have been created to reflect the configuration of the network to allow only authorised devices to connect to the wired and wireless network. For example, NAC / 802.1x has been configured by CGI to allow only authorised CEC devices to connect to the network.
Availability aspects of network security	Access management	● The network devices are configured in such a way that: ○ default passwords are changed on all network devices; ○ role based access and appropriate access levels are assigned on the network devices based on the user's necessary level of access; ○ principle of least privilege and default deny is enforced on all devices; and ○ elevated access privileges are provided only to members of staff approved by senior management. ● Access to the network devices including level of access is recertified and reviewed regularly. ● Remote access to the network and network devices is reviewed and ensured to be sufficiently controlled.
	Network redundancy and identification of assets	● Network controls and equipment are configured to provide high availability and a level of redundancy to avoid single point of failure on the network. ● Fail safe and failover mechanisms are defined and secondary connections have been configured to ensure high availability. ● Failure modes are documented and tested periodically, including the effectiveness of shifting to the secondary network devices.

The City of Edinburgh Council

Internal Audit

Arm's Length External Organisations (ALEO)

Final Report

2nd August 2021

CW2001

Overall report rating:

Significant Improvements 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.

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2020/21 internal audit plan approved by the Governance, Risk and Best Value Committee in September 2020. 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 a number of 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.

1. Background and Scope

Background

Arm's Length External Organisations

Audit Scotland describes Arm's Length External Organisations (ALEOs) as organisations that are 'formally separate to the Council but are subject to its control or influence.' Ownership, provision of funding, and significant shareholdings in a company all constitute significant control or influence, and therefore constitute an arm's length relationship with external organisations.

The Council is responsible for ensuring that Audit Scotland's 'Following the Public Pound' principles are consistently applied by any ALEOs that it provides funding to, and must ensure that ALEOs can demonstrate value for money.

Reporting arrangements for ALEOs will vary depending on the structure of each entity for example, Limited Liability Partnerships; Limited Companies; Charities; and Charitable Trusts. However, the Council has a duty to include details of the financial performance of any ALEOs where it holds a controlling interest, in its annual accounts.

The Standards Commission Scotland (the Commission) is an independent body responsible for encouraging high ethical standards in public life through the promotion and enforcement of Codes of Conduct for Councillors and those appointed to the boards of devolved public bodies.

The Commission's July 2018 Code of Conduct for Councillors includes a section on Appointments to Partner Organisations that confirms Councillor's responsibilities to declare any potential conflicts of interest where they have been appointed as a director of a company or a charitable trust as a nominee.

The following external reports and guidance is also available to support Council's with their ongoing governance and scrutiny of ALEOs. These include:

- Council's Use of Arm's Length Organisations - Audit Scotland (2018)
- Advice for Councillors on arm's Length External Organisations - The Standards Commission for Scotland (2016);
- Inquiry into Arm's Length External Organisations - Scottish Parliament (2016)
- Arm's Length external organisations (ALEOs): are you getting it right? - Audit Scotland (2011); and
- Report on Arm's Length External Organisations - Office of the Scottish Charity Regulator (2015).

Council ALEOs

Details of ALEOs where the Council has an established interest or relationship are maintained on a register. The current version of the register (June 2019) confirms that the Council has arm's length relationships with 30 external organisations and 37 associated subsidiary companies that deliver a varied range of services including the provision of public transport services; leisure facilities; cultural venues and trusts; property development; pension investment and management.

Each ALEO is aligned with a relevant Council directorate and should have established service level and / or funding agreements in place that cover any services delivered to or received by the Council and any funding provided by the Council.

Current governance arrangements

A Council Governance Hub chaired by the Chief Executive was established in 2016 to scrutinise delivery of services by ALEOs; to ensure that the Council is aware of any new and emerging risks; confirm the ongoing independence of elected members as directors of ALEOs; review ALEO annual assurance statements; and confirm that there is adequate ongoing reporting by ALEOs to both Council executive committees and the Governance, Risk and Best Value Committee. The Hub also provides an opportunity for ALEOs to raise any issues or concerns directly with the Council.

To support the Council's ongoing scrutiny of ALEOs, Council Officers are appointed as independent observers at ALEO boards. The Council Observer (CO) is essentially a representative of the Council with no voting rights, and attends meetings to confirm ongoing compliance with any agreements between the Council and the ALEO, and to identify any potential risks to the Council. Observers should escalate any immediate concerns to their line manager.

The Council also requires elected members to declare any potential conflicts of interest, and these are recorded and maintained in a register. Any relevant conflicts of interest are also declared at the beginning of any Council executive committee meetings, including the Governance, Risk and Best Value Committee.

The Corporate Governance section of the Council's 2018 financial statements (refer page 145) included two actions (actions 11 and 13) to improve governance arrangements in relation to ALEOs. These were:

- Reporting of ALEOs has gone to executive committees and the Chief Executive but not all ALEOs are also reporting to the Governance, Risk and Best Value Committee. Work will be undertaken with directors and the Governance Hub to improve awareness and compliance with the reporting process
- A review of arrangements is underway to ensure ALEOs have a service level agreement or funding agreements.

Future Governance Arrangements

A paper titled Arms' Length External Organisations – Reporting to Committee was presented to the Council's Policy and Sustainability Committee in February 2020 that outlines a revised reporting approach for ALEOs to relevant Council Committees. This included proposals for:

- Council Executive Committees to scrutinise ALEO future direction; performance and service delivery; and progress against relevant agreements (including service level agreements)
- The Governance, Risk, and Best Value Committee to scrutinise ALEO financial performance, and risks.
- Reports to include annual financial statements and a section prepared by the Council's observer detailing any comments they have in relation to performance and risk management.
- Representatives from the ALEO's executive management team and the Council observer to be present at committee for consideration of the reports.

Various papers have also been presented to the Council's Committees in relation to the reform of Transport ALEOs. A report to Policy and Sustainability Committee in July 2020 highlighted the current arrangements and challenges for the management of the Council's Transport ALEOs. In November 2020, the Transport and Environment Committee established a short life working group to develop a preferred governance and operating structure for delivery of Council owned public transport.

Previous Assurance Reviews

ALEO governance arrangements was last reviewed by Internal Audit (IA) in April 2016. This review included 1 High and 3 Medium rated findings highlighting that:

1. High - Councillors who are both legal directors of an Arm's Length Company and sit on the scrutinising committee for that entity could be perceived as having a conflict of interest as they may be scrutinising actions that they as directors are responsible for.
2. Medium - Council Observers for EICC & EDI are not attending all the Board or Audit Committee meetings. In addition, we did not identify process documentation for the Council Observer role in any of the Service Directorates.
3. Medium - The Council's annual assurance questionnaire process would benefit from tailoring to ensure that it meets the needs of Arm's Length Companies.
4. Medium – Arm's Length Companies are not always subject to regular scrutiny by the relevant scrutiny Committee.

Additionally, a number of external assurance reviews were completed by the Accounts Commission (2011; 2015; and 2018); and the Office of the Scottish Charity Regulator (OSCR) in 2015.

The conclusions drawn from each of these reviews were that further work was required to realise benefits from ALEOs whilst managing the associated risks, with a number of improvement identified in each review.

Covid-19 Impact on ALEOs

The Covid-19 pandemic has adversely impacted both the operation and financial performance of the majority of the Council's ALEOs as a number of services that they provide (for example cultural venues and leisure activities) have either been closed, or have been subject to a significant decrease in demand (for example transport services) since March 2020.

This will also adversely impact the Council's current and future financial position as ALEOs are unlikely to be able to deliver expected financial returns (for example annual dividend income received from Lothian buses) and may require additional future funding and support to reinstate their services.

It is therefore essential to ensure that ALEOs have taken advantage of all Scottish Government grant funding and support schemes available to them; have accurately recorded the risks and associated impacts on performance (both financial and non-financial; have established appropriate recovery plans; and that the Council has reviewed and scrutinised the approaches adopted by each ALEO.

Scope

The objective of this review is to assess the adequacy of design and operating effectiveness of the Council's established governance and scrutiny arrangements (including appropriate risk management arrangements and Covid-19 impacts and recovery plans) in relation to its ALEOs during the period 1 April to 31 December 2020.

Approach

The following approach was applied across a sample of ten Council ALEOs to support completion of the review:

- Identify the key risks in relation to ensuring the Council has established adequate and effective governance arrangements in relation to its ALEOs;
- Identify the key controls established to mitigate these risks;

- Evaluate the design of the key controls in place to address the key risks. This will involve discussions with elected members and officers appointed to ALEO Boards and also independent observers.
- Assess the operating effectiveness of the key controls;
- Prepare a draft report detailing the findings raised and Internal Audit recommendations;
- Discuss all control gaps identified and agree management actions with key stakeholders at a workshop; and
- Prepare a final report detailing that includes agreed management actions and implementation dates.

Limitations of Scope

There are no specific scope limitations.

Reporting Date

Our audit work concluded on 3 March 2021 and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 2

Summary of findings raised	
High	1. ALEO Governance Framework
High	2. Conflicts of Interest, Appointments, and Training

Opinion

Our review identified a number of significant control weaknesses in the design and effectiveness of the Council's Arm's Length External Organisations (ALEOs) governance, control, and risk management arrangements. Consequently, only limited assurance can be provided that the risks associated with ALEOs are being managed, and that the Council's objectives of effectively managing and scrutinising ALEO operational performance and risk management processes should be achieved.

Over the years the Council has implemented a number of measures to address the findings raised in previous internal and external ALEO assurance reviews. These include establishing the Governance Hub and providing guidance for Council Observers (2016); clarifying ALEO oversight measures (2018); and more recently (February 2020), approving the refreshed reporting approach to both relevant executive committees and the Governance, Risk and Best Value Committee (GRBV).

However, our review has confirmed that further work is required to strengthen the Council's ALEO governance and risk management arrangements, and ensure that they are consistently applied as management actions implemented to address findings raised in relation to potential conflicts of interest and the role of Council Observers raised in previous assurance reviews have not been sustained.

The annual governance statement (AGS) included in the Council's 2019/20 financial statements also reinforced that the division of scrutiny of the Council's Arm's Length External Organisations (ALEOs) between executive committees and Governance, Risk and Best Value Committee is essential to ensure that potential conflicts of interest are mitigated; confirmed that separation of scrutiny has not always been clear, and that duplication of scrutiny has been common.

Whilst the arrangements included in the Arms' Length External Organisations – Reporting to Committee paper that were agreed by the Council's Policy and Sustainability Committee in February 2020 should have addressed this concern, our review has confirmed that these have not been consistently and effectively applied.

Consequently, 2 new High rated findings have been raised.

The first High rated finding reflects the fact that the current operational management of ALEOs by the first line is not consistent. Accordingly, there is a need to establish a second line ALEO governance framework that should be applied by first line directorates to ensure consistent and effective ongoing governance and scrutiny of ALEOs, as various inconsistent approaches are currently being applied. This finding also highlights the need to ensure that centralised ALEO details are consistently maintained and reviewed, and the importance of confirming the ongoing financial feasibility of ALEOs as the economic and financial impacts associated with Covid-19 become clearer.

Our second high rated findings reinforces the need to ensure that potential or perceived conflicts of interest in relation to Elected Member appointments to ALEOs are considered and addressed in line with Audit Scotland requirements; and the importance of ensuring that both Elected Members and Council Observers involved with ALEOs have relevant and appropriate skills and experience and complete appropriate training in line with relevant Audit Scotland guidance.

Further detail on these findings is included at Section 3.

3. Detailed findings

1. ALEO Governance Framework	High

Review of the processes established by the Council to support management and scrutiny of Arm's Length External Organisations (ALEOs) confirmed that:

1. **ALEO governance framework** - there is currently no established ALEO governance framework that provides a consistent second line approach to the establishment and ongoing management of ALEOs that can be applied across the Council by first line directorates.
2. **First and second line roles and responsibilities** – second line responsibilities for developing and maintaining an ALEO governance and management framework and first line directorate responsibilities for its consistent application have not been clearly defined and agreed.

   It is acknowledged that the Democracy, Governance, and Resilience (DGR) team currently performs elements of this second line role on an ad hoc basis (when required) by drafting service level; funding; or shareholder agreements, or supporting queries about establishing new ALEOs, however, DGR has advised that they are not currently empowered or resourced to perform a second line ALEO oversight or scrutiny role.

At the time of our review, DGR was in the process of developing guidance for incorporating a council company.

3. **Governance Hub –** Following a report to Council in June 2016, the governance hub was established in Oct 2016 with the objective of scrutinising and reporting ALEO performance and identifying and reporting any significant risks to the Council. Review of the operation of the governance hub established that:

   - the protocols for determining which ALEOs should attend the Governance Hub have not been documented.
   - the purpose of the governance hub has evolved over time from its originally agreed terms of reference.
   - whilst a standing agenda exists and meeting minutes are prepared, there is no formal action tracker that records agreed decisions, responsibilities, and completion timeframes, and progress with agreed actions is monitored informally.

4. **Inconsistent approaches –** lack of an established ALEO governance and management framework has resulted in various inconsistent approaches being applied to the governance of ALEOs across the Council.

   Whilst some variances would normally be expected given the differences in structure, size and risks associated with each ALEO significant variances were identified.

   Of the 30 external organisations and 37 associated subsidiary companies listed as ALEOs in the current version of the central ALEOs register (June 2019):

   - Only 7 ALEOs are represented in the Governance Hub. It is acknowledged that it may not be appropriate for all ALEOs to be included in the Governance Hub, however criteria for inclusion has not yet been defined
   - Fewer than 10 ALEOs report performance updates to Council committees;
   - Fewer than 20 ALEOs have Council Observers appointed; and
   - Fewer than 25 ALEOs have elected members of Council appointed to their board.

5. **Council Observer (CO) Reports** - ALEO reports provided to Council Committees are not currently supported by reports from COs in line with the revised ALEO reporting approached agreed by the Policy and Sustainability Committee in February 2020.

6. **Central ALEO register** – DGR currently maintains a centralised ALEO register that includes details of Council Observers (Cos); Elected Members (EMs); lead directorates; and details of any established service and funding agreements.

   Review of the current register established that it has not been recently updated. Specifically:

   - First line directorate responsibilities for ALEOs relationship management have not been consistently recorded.
   - EMs for Capital Theatres, Capital City Partnership and Marketing Edinburgh are not recorded in the register, but are documented in a separate master spreadsheet.
   - the lead officer for each ALEO has not been updated, for example, the Chief Executive for Marketing Edinburgh Limited and for EDI Group Limited.

7. **Ongoing review of the central ALEO register** - whilst a process has been established by DGR to update the ALEO register when notified of a change by Companies House, there is currently no

regular scheduled review of the centralised ALEO register maintained by the DGR team to confirm that it remains up to date.

8. **Financial Sustainability** - in response to Covid-19, the Council's 7 high risk ALEOs were requested to prepare detailed financial scenarios for the next 12 months (2021-22). Whilst this was reported to the Corporate Leadership Team and considered by the Governance Hub, there are currently no plans to request further detailed financial scenarios for review.

Risk

The potential risks associated with our findings are:

- **Regulatory and Legislative Compliance -** management and scrutiny of ALEOs is not performed consistently across the Council by the first line as agreed and in line with relevant Audit Scotland; Standards Commission; Scottish Parliament; and Office of the Scottish Charity Regulator regulations and guidance.
- **Governance and Decision Making** Significant ALEO performance issues and risks may not be identified and addressed.
- **Service Delivery –** lack of clear understanding in relation to the nature and quality of services provided to and from ALEOs by the Council.
- **Financial and Budget Management –** the Council does not have a clear picture of future ALEO financial sustainability and its potential impact on both Council services and finances.
- **Reputational Risk –** adverse publicity associated with ALEO operational performance and service delivery.

1.1 Recommendation: ALEO Governance Framework

1. Second line responsibilities for the design, implementation, and ongoing maintenance of an ALEO governance framework should be agreed.
2. An ALEO governance framework should be designed and implemented. This should include (but not be limited to):
    - A clear definition of Council ALEOs
    - A refreshed terms of reference for the Governance Hub that details who should attend and outlines the governance processes to be applied (where relevant) in meetings;
    - Definition of criteria for ALEOs that should be included in the Governance Hub;
    - Clear allocation of an ALEO or group of ALEOs to first line directorates;
    - Roles and responsibilities for first line directorates and Council Observers (COs);
    - Roles and responsibilities for Elected Members (EMs) including the process to be applied when they are appointed to ALEO boards;
    - Guidance on how ALEO management and scrutiny responsibilities should be performed by both COs and EMs;
    - Standard templates for service level and funding agreements that can be completed by first line teams;
    - ALEO and CO operational performance and risk management reporting requirements to both Council Executive Committees and the Governance, Risk, and Best Value Committee.

- Details of the ongoing central ALEO register maintenance responsibilities, including responsibilities for providing details of changes to be included, and responsibility for confirming its ongoing completeness and accuracy; and
- First and second line assurance responsibilities in relation to the ongoing management and oversight of ALEOs.

3. The governance framework should be communicated across the Council to all first line teams (including COs) and EMs involved in management and scrutiny of ALEOs. This should be supported by training where required.

1.1 Agreed Management Action: ALEO Governance Framework

1. Second line responsibilities for the design, implementation, and ongoing maintenance of an ALEO governance framework will be agreed; and
2. An ALEO governance framework will be designed implemented, and communicated that incorporates all of the recommendations above.

Owner: Stephen Moir, Executive Director of Corporate Services **Contributors:** Nick Smith, Service Director: Legal and Assurance; Gavin King, Head of Democracy, Governance and Resilience; Laura Callender, Governance Manager; Ross Murray, Governance Officer; Layla Smith, Operations Manager, Corporate Services, Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 30 Sept 2022

1.2 Recommendation: Central ALEO Register

1. The central ALEO register should be reviewed and updated, with confirmation obtained from directorates of the location of relevant supporting documents (for example service and funding agreements).
2. Ongoing review of the central ALEO register should be implemented at an appropriate frequency (for example every six months) to confirm that it remains complete and accurate.

1.2 Agreed Management Action: Central ALEO Register

The recommendations detailed above will be implemented.

Owner: Stephen Moir, Executive Director of Corporate Services **Contributors:** Nick Smith, Service Director: Legal and Assurance; Gavin King, Head of Democracy, Governance and Resilience; Laura Callender, Governance Manager; Ross Murray, Governance Officer; Layla Smith, Operations Manager, Corporate Services, Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 16 December 2022

1.3 Recommendation: ALEO Financial Sustainability

1. Existing quarterly monitoring reports for high risk ALEOs should be updated to include the potential service delivery and financial impacts associated with new and emerging and ongoing ALEO financial risks, including the ongoing impacts of Covid-19).
2. The reports should be reviewed by the Corporate leadership Team (CLT); the Governance Hub; and relevant Executive Committees (as required) to ensure that both service delivery and financial issues and risks have been identified, and appropriate action plans established.

1.3 Agreed Management Action: ALEO Financial Sustainability

Recommendation accepted. Engagement with ALEOs will continue, with the potential service delivery and financial impacts associated with new and emerging and ongoing ALEO financial risks incorporated into the Council's established quarterly monitoring reporting process.

These reports are currently provided to the Corporate Leadership Team; the Finance and Resources Committee; and will also be provided to the Governance Hub.

Owner: Stephen Moir, Executive Director of Corporate Services **Contributors:** Hugh Dunn, Service Director, Finance and Procurement; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 31 March 2022

1.4 Recommendation: Implementation of ALEO Framework by Directorates

1. Following design, communication and delivery of training on the ALEO governance framework, directorates should ensure that it is implemented and consistently applied to their relevant ALEO relationships.
2. Directorates should also design and implement their own first line assurance activities to confirm that the ALEO framework is being consistently applied, and will take appropriate steps to address any significant variances identified.

1.4a Agreed Management Action: Implementation of ALEO Framework by Place

The new ALEO Governance framework will be implemented within the Place Directorate for those organisations which are defined as an ALEO and for which Place is responsible for the on-going relationship.

This will include Edinburgh Leisure which currently sits within the Education and Children's Services Directorate and will transfer across to the Place Directorate at a future date to be confirmed.

Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Service Director – Operational Services, Peter Watton, Service Director - Sustainable Development, and Service Directors for Housing, Family Support and Fair Work and Culture and Wellbeing; Operations Manager;	**Implementation Date:** 30 September 2023.

1.4b Agreed Management Action: Implementation of ALEO Framework by Corporate Services

Recommendations accepted and will be implemented following the rollout of the governance framework at a corporate level. This will also be factored into and considered as a part of first line managerial responsibilities across Corporate Services and as part of first-line assurance arrangements which are in the process of being introduced and should be embedded by the time this framework needs rolled out.

Owner: Stephen Moir, Executive Director of Corporate Services **Contributors:** Nick Smith, Service Director: Legal and Assurance; Gavin King, Head of Democracy, Governance and Resilience; Laura Callender, Governance Manager; Ross Murray, Governance Officer; Layla Smith, Operations Manager, Corporate Services, Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 30 September 2023

2. Conflicts of Interest, Appointments, and Training — High

1. **Conflicts of Interest** - we identified 5 instances where EMs on the board of ALEOs also sat on the relevant Council executive committee responsible for scrutiny and oversight of the ALEOs performance. This issue was also previously highlighted in the April 2016 Internal Audit report.

   It is acknowledged that these conflicts may have been highlighted by EMs through the established declaration process when ALEO performance reports were presented to the Council committees for scrutiny.

2. **Elected Member (EM) appointments –** there are currently no established protocols that clearly define the basis for EM and CO appointments to ALEO boards that considers alignment of their skills, experience, and background and clearly defines their roles and responsibilities.
3. **Regular review of ALEO appointments** – no review process has been established to confirm that EM's appointed to ALEOs continue to be the most suitable fit for the role.
4. **Training** – review of training available to both Elected Members (EMs) and Council Observers (COs) involved in ALEOs confirmed that:
   - only code of conduct training is classified as mandatory for EMs, whilst completion of training on director's duties and appointment to outside bodies remains voluntary.
   - training records are not maintained for COs and were incomplete for EMs, as we were unable to confirm whether 9 out of 20 EMs had completed training.

Risk

The potential risks associated with our findings are:

- **Regulatory and Legislative Compliance –** conflicts of interest are not identified and managed in line with Audit Scotland requirements.
- **Regulatory and Legislative Compliance –** Elected Members (EMs) appointed to ALEO boards may not have relevant skills and experience as recommended in Audit Scotland guidance

- **Governance and Decision Making** – poor governance and decision making occurs as EMs and Council Observer (CO) skills gaps are not addressed by completion of relevant training as also recommended in Audit Scotland guidance.
- **Reputational Risk –** adverse publicity associated with potential conflicts of interest and ineffective governance.

2.1 Recommendation: Conflicts of Interest and Appointments

1. Management should consider and confirm whether they are prepared to accept the reputational risks associated with perceived conflicts of interests where Elected Members (EMs) on ALEO boards also sit on the relevant Council executive committees responsible for ALEO scrutiny, and document the outcomes of this decision. Audit Scotland requirements and guidance should be considered as part of this decision making process
2. Where this risk is accepted, the supporting rationale should be recorded in relevant risk registers.
3. Established conflict of interest procedures should be reviewed and refreshed to align with the outcome of the decision noted at point 1 above, and communicated to all Elected Members.
4. The skills, background and experience required for EMs appointed to ALEO boards and Council Observers (COs) who represent the Council's interest at board meetings should be considered; documented; and consistently applied in the ALEO Board appointment process (refer recommendation 1.1 above). This should include consideration on continuing professional development requirements where this is considered appropriate.
5. Skills and experience of both EMs and COs should be reviewed at appropriate intervals to confirm that it remains relevant to support effective discharge of the responsibilities associated with these roles.

2.1 Agreed Management Action: Conflicts of Interest and Appointments

1. and 3 The Democracy, Governance, and Resilience (DGR) team has introduced an ALEO scrutiny process where ALEOs are scrutinised by both relevant executive committees (where conflicts of interest could exist) and the Governance, Risk and Best Value Committee (where no conflicts should exist) to further mitigate this risk.

   It is acknowledged that as fewer than ten ALEOs currently report performance updates to Council committees (as highlighted in finding 1), further clarity is needed to confirm that these include all ALEOs where potential EM conflicts of interest exist in relation to executive committee scrutiny.

   At the beginning of every new Council term Elected members are allocated to ALEOs, and it is expected that these appointment will remain in place for the duration of the five year Council term.

   Following the allocation of EMs to ALEOs, a paper will be prepared and presented to full Council that highlights any potential conflicts of interest between ALEO and Council committee appointments (including the Governance, Risk, and Best Value Committee), with a request that the Council either risk accepts or takes action to address the potential conflicts identified.

   This report will also highlight that future potential conflicts could occur if EM appointments to either ALEOs or Council committees are changed, and that this should be considered by political groups as part of any subsequent appointment changes.

2. It is acknowledged that the risks associated with potential EM ALEO conflicts of interest should be recorded and noted as having been risk accepted as part of the Council's risk management framework, together with supporting rationale.

   Following presentation of the paper to full Council noted above, Executive directors will be advised of any potential ALEO conflicts of interest that have been risk accepted and requested to ensure that these are reflected in relevant risk registers.

4. A framework will be designed and provided to all ALEOs that makes recommendations for an appropriate composition of both elected members and independent members for inclusion in ALEO boards to ensure that there is an appropriate balance and mix of skills.

   The skills, background and experience required for Council Observers (COs) who represent the Council's interest at board meetings will be considered; documented; and consistently applied to all appointments.

5. The DGR team will send reminders to each Group annually about the recommendation that there be an appropriate composition of both elected members and independent members for inclusion in ALEO boards. Each Directorate will be asked by DGR to confirm (at least annually) that the background, skills and experience of each CO remains appropriate.

Owner: Stephen Moir, Executive Director, Corporate Service **Contributors:** Nick Smith, Service Director, Legal and Assurance; Gavin King, Head of Democracy, Resilience and Governance; Laura Callender, Governance Manager; Ross Murray, Governance Officer; Layla Smith, Operations Manager, Corporate Services, Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 30 June 2023

2.2 Recommendation: Training

1. Existing training materials for both Elected Members (EMs) and Council Observers (COs) should be reviewed and refreshed to ensure there is sufficient information on managing ALEOs, including legal responsibilities, scrutiny and oversight, and conflicts of interest, and any recent updates from regulatory bodies such as Audit Scotland; The Standards Commission; the Scottish Parliament; and the Office of the Scottish Charity Regulator.
2. Training materials should be regularly reviewed to confirm that their content remains relevant.
3. Management should consider making training mandatory for both EMs and COs with the requirement to complete refresher training at appropriate intervals (for example, annually). Where training is not mandated, it should be promoted and the need for completion regularly reinforced with both groups.
4. Training records should be established, maintained, and regularly reviewed to confirm completion, with follow up performed where training has not been completed.

2.2 Agreed Management Action: Training

1. and 2 Agreed. Actions will be implemented as recommended.

3. It was agreed at a meeting of full Council in June 2016 that EMs who were directors of Council companies would undertake mandatory training on their duties under the Companies Act. Training will also be made mandatory for COs. 4. Completion of training by both EMs and COs will be monitored and where training has not been completed, Group Leaders will be notified.	
Owner: Stephen Moir, Executive Director, Corporate Services **Contributors:** Nick Smith, Service Director, Legal and Assurance; Gavin King, Head of Democracy, Resilience and Governance; Laura Callender, Governance Manager; Ross Murray, Governance Officer; Layla Smith, Operations Manager, Corporate Services, Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 30 June 2023

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation of the organisation which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation of the organisation.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the organisation.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Please see the Internal Audit Charter for full details of opinion ratings and classifications.

Appendix 2: Areas of audit focus

The areas of audit focus and related control objectives included in the review were:

Audit Area	Control Objectives
Strategy and Communications	1. The Council has a clear definition of ALEOs and applies this consistently to external organisations that it deals with to determine whether they should potentially be classified as ALEOs. 2. The role of Council independent observer on ALEO Boards has been clearly defined. This should include but not be limited to: • monitoring ongoing compliance with any agreements between the Council and the ALEO, including compliance with funding requirements; • review of Board papers to identify any potential operational and financial performance concerns and identification of any potential risks to the Council. • Annual reporting to the Governance Hub (GH); and • escalation of any immediate concerns to their line manager. 3. Guidance has been provided to Directorates and Divisions on ongoing management of ALEOs that includes the requirement to: • consider whether any new relationships with external organisations should be classified as ALEOs; • advise Strategy and Communications and also the GH of any new ALEO arrangements; • ensure that appropriate service level agreements have been established detailing services provided to or received from the ALEO and are regularly reviewed; • ensure that appropriate annual funding agreements supported by appropriate funding conditions have been established where funding is provided by the Council to ALEOs; • ensure that appropriate ALEO relationship managers (at Directorate or Head of Service level) have been established and independent observers appointed to ALEO Boards; and • ensure that ALEO performance and annual governance statements are reviewed by the GH and the appropriate Council executive committees (including the Governance, Risk and Best Value Committee). 4. The ALEO register is circulated to Directorates at an appropriate frequency to confirm that all current ALEOs are included; that SLAs and funding agreements are in place; and that ALEO performance has been scrutinised at relevant Council executive and the Governance, Risk and Best Value Committee.

Governance Hub	1. Terms of reference has been established and shared with Council ALEOs that details the role, responsibilities and accountabilities of the Governance Hub (GH) and its ongoing engagement with ALEOs. These should include, but should not be limited to ongoing oversight of ALEO: • board composition to ensure that there are no potential conflicts of interest; • strategic planning and decision making; • operational and financial performance; • risk management; • assurance outcomes; • annual governance statements; • financial statements; • reporting to relevant Council executive and Governance, Risk and Best Value Committees; and • annual reports prepared by Council independent observers and any issues raised and escalated to the GH. 2. The GH is also responsible for assessing any new relationships with external organisations to determine whether these should be classified as ALEOs for inclusion in the register and potentially the Council's annual financial statements. 3. GH membership has been clearly defined, including representation from ALEOs. 4. Regular GH meetings are scheduled and are supported by agendas that are aligned with its terms of reference. 5. Actions from GH meetings are allocated to appropriate members with agreed timelines for completion, and implementation progress monitored at subsequent GH meetings. 6. Changes outlined in the January 2020 paper provided to the Policy and Sustainability Committee have been effectively implemented.
Directorates and Independent Observers	1. All new relationships established with external organisations have been assessed to consider whether they should be classified as ALEOs, with Strategy and Communications requested to update the central ALEO register and the GH advised where this is the case. 2. ALEO relationship management responsibilities have been allocated at an appropriate level (Director or Head of Service) and independent observers appointed to each ALEO Board. 3. Service level agreements detailing the services to be provided to or from the Council by the ALEO have been established and are supported by key performance indicators (where appropriate), with performance regularly monitored. 4. Funding agreements (supported by relevant funding conditions) have been established with ongoing compliance with funding conditions regularly monitored.

Training and Guidance	1. There are clear guidelines for elected members and officers who are appointed to the board of an ALEO, including guidelines covering conflicts of interest 2. Training is provided to elected members and officers appointed to ALEO Boards on how to perform effective scrutiny and how to identify and report any potential conflicts of interest. 3. Council observers receive adequate training and guidance to enable them to carry out their role effectively
Councillor Appointments	1. The Council appoints elected members and officers to the boards of ALEOs with reference to their skills and experience. 2. Conflicts of interest are effectively managed by ensuring that elected members do not sit on the board of ALEOs and the relevant Council executive committee responsible for scrutiny and oversight of the ALEOs performance (including the Governance, Risk and Best Value Committee). 3. The Council ensures that there is at least one elected member or Council officer on the board of each ALEO.
Covid-19 Impacts	1. The Council has obtained evidence from ALEOs confirming that they have: • taken advantage of all available Scottish Government grant funding and support schemes available to them. • identified all relevant Covid-19 risks; assessed and recorded them; and taken appropriate action to mitigate them where possible. • accurately monitored both the financial and non-financial impacts of Covid-19 on their services, and • Established appropriate service recovery plans 2. The Council has monitored the financial impact associated with reduced income from ALEOs, and reflected this in future financial plans (the Council's budget is due to be completed in February 2021). 3. Appropriate scrutiny has been applied to ALEO recovery plans by both senior management and relevant Council Executive Committees to confirm that they are realistic and achievable, and can be immediately implemented when permitted by the Scottish Government.

The City of Edinburgh Council

Internal Audit

Education and Children's Services

Health and Safety – Managing Behaviours of Concern

Final Report

2nd August 2021

CF2003

Overall report rating:

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.

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2020/21 internal audit plan approved by the Governance, Risk and Best Value Committee in September 2020. 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 is a number of 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.

1. Background and Scope

Background

The Health and Safety Executive (HSE) is an independent regulator for work-related health and safety in the UK and defines work-related violence as: "any incident in which a person is abused, threatened or assaulted in circumstances relating to their work", and has produced guidance on Violence at Work for employers.

The City of Edinburgh Council (the Council) has 122 primary, secondary and special schools and employs 3,372 teachers to provide educational services to 63,115 children between the ages of 5-17.

These schools are managed in line with the Council's devolved school management scheme that was designed and implemented in response to the principles established under the June 2018 Joint Agreement between the Scottish Government and COSLA and the Scottish Government's Devolved School Management Guidelines that empower headteachers in relation to curriculum, improvement, staffing and funding.

Behaviours of Concern Legislative and Regulatory Requirements

Any form of concerning behaviour by pupils towards teachers and other staff members at the Council operated educational establishments is governed by the regulations detailed below, and the Council's Violence at work and Health and Safety policies are designed to ensure compliance with these regulations and alignment with HSE guidance.

- The Health and Safety at Work etc. Act 1974 (HSW Act);
- The Management of Health and Safety at Work Regulations 1999;
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR);
- The Safety Representative and Safety Committees Regulations 1977 (a); and
- The Health and Safety (Consultation with Employees) Regulations 1996 (b).

The Council's Health and Safety Policy sets out requirements and roles and responsibilities for the management of Health and Safety risks including behaviours of concern. Line managers are required to manage and investigate any incident of concerning behaviour and to report it through the Corporate Health and Safety online 'SHE' Assurance Portal.

The Corporate Health and Safety (H&S) team reviews all incidents reported on the SHE Assurance Portal and identifies those incidents which meet the RIDDOR category requirements which require to be reported to HSE. The H&S team leads in the investigation and reporting of this incident classification.

It is understood that the SHE Assurance Portal is in the process of being updated with system improvements in particular to how incidents are classified and that the new version of the portal was rolled out on 01 July 2021.

Incidents are classified as work related accident / ill health; near miss; non–work related incidents; and pupils and service users on the SHE Assurance Portal.

Quarterly Health and Safety dashboards are produced by the Corporate Health and Safety Team and presented to the Communities and Families Health and Safety Group. Council-wide dashboards are also presented quarterly and annually to the Council's Health and Safety Group, and health and safety performance is also measured and reported quarterly to the Directorates Risk Committees.

Policies, Procedures and Training

The following Council policies and procedures detail how behaviours of concern should be managed across the Council:

Corporate Policies and Procedures:

- Violence at Work Policy
- Violence at Work Toolkit
- Violent Incident Reporting Flowchart (linked to Toolkit document).

Corporate Health and Safety Policy and Procedures:

The following policies can be found on the ORB:

- Council's Health and Safety Policy
- Incident Reporting - Guidelines for managers and employees
- Step by Step guide on reporting incidents on the SHE Assurance Portal.

Education and Children's Services (Formerly Communities and Families {C&F}) Policy and Procedures:

- Included, Engaged and Involved in Edinburgh
- Managing and Reducing Risk
- Relationships, Learning and Behaviour

Training

Schools are very much focused on preventing behaviours of concern and promoting positive relationships and behaviours.

Consequently, whole School autism training is mandatory for primary, secondary and special schools and it is understood that this training should be completed every three years.

The Promoting Positive Relationships for Learning and Positive Behaviour eLearning module is held on the Council's CECiL system which links into the Relationships, Learning and Behaviour procedure. This module has not been classified as mandatory or essential learning.

The Corporate Health and Safety team has rolled out 'bitesize' health and safety courses from early June 2021, including incident reporting on the SHE Assurance Portal, and Understanding RIDDOR Investigations.

Scope

The objective of this review was to assess the adequacy of design and operating effectiveness of the key controls established to ensure the Council has established appropriate processes and provided adequate training to all educational establishment employees to enable them to defuse and manage behaviours of concern exhibited by pupils.

Further details of our areas of audit focus are included at Appendix 2.

Our work was completed through engagement with a number of managers within Education and Children's Services (formerly C&F); and the Council's Health and Safety and Learning and Development teams.

Four schools (two primary Schools; one secondary; and one special school) were selected to complete walkthroughs of the incident reporting process.

Recognising the ongoing challenges associated with Covid-19, only two primary schools were able to support full walkthroughs. Our testing was further supported by discussions with the following employees:

- Three Head Teachers,

- Two Business Managers,
- One PSA
- One Teacher

Testing was undertaken on a sample basis for the period 01 April 2020 to 31 December 2020.

Limitations of Scope

Following review of reported incidents across establishments within Education and Children's Services, our scope was limited to primary, secondary, and special schools, and did not include Council and partner provided nurseries and early years establishments; young persons' centres / secure accommodation units; community centres; outdoor education centres; and libraries.

Reporting Date

Our audit work concluded on 21st May 2021, and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 3 and 1 Advisory

Summary of findings raised	
High	1. Policies and Procedures
High	2. Employee Induction and Training
Medium	3. Governance and Management Information
Advisory	4. Health and Safety – Incidents Reported to the Health and Safety Executive

Opinion

Significant Improvement Required

Our review identified significant and numerous control weaknesses in both the design and effectiveness of the control environment and governance and risk management frameworks established within Education and Children's Services (formerly C&F) and individual schools to both prevent and manage the occurrence of behaviours of concern (BoC) incidents.

Consequently, only limited assurance can be provided that BoC health and safety risks that could impact both pupils and employees are being managed, and that the Council's objectives of defusing and effectively managing concerning behaviours should be achieved.

Whilst it is acknowledged that the Council's schools are empowered under the devolved school management scheme, it is our opinion (based on our findings) that ongoing management of BoC health and safety risks is one area where greater synergy and consistency would be achieved by adopting a centralised approach, which should also confirm ongoing compliance with applicable legislation and regulations.

It is also important to note that whilst the scope of our review was limited to schools, the findings raised in this report could potentially be relevant to other areas of the Council.

Reported Incidents

Our opinion is supported by the circa 370 incidents recorded in the SHE incident reporting system by Schools and Lifelong learning between May 2020 and February 2021 that can be analysed as follows:

- 68% - physical assault by a person with additional support needs for learning
- 18% - threatening; aggressive; challenging behaviour including physical abuse
- 12% - physical assault by another type of person

Findings Raised

Consequently, two high and one medium rated findings have been raised that highlight the need to:

- ensure that the Council's Violence at Work policy is refreshed and communicated (finding 1);
- review and refresh Education and Children's Services policies and procedures in relation to preventing and managing BoC incidents and ensure that they are consistently applied (finding 1);
- ensure that appropriate complaints and escalation procedures are established to support employees who have concerns about how BoC incidents are being managed (finding1);
- ensure that lessons learned are identified, recorded, and incorporated into risk assessments and pupil plans where appropriate (finding 1);
- refresh the content of Education and Children's Services preventative and incident management training, and ensure that this is consistently completed (finding 2);
- ensure that Pupil Support Assistants (PSAs) have sufficient capacity within their contracted working hours to complete their training (finding 2); and
- confirm governance arrangements for ongoing management review and oversight of incidents, ensuring that appropriate actions are implemented to prevent recurrence of any potentially significant and thematic incidents (finding 3).

One opportunity to improve the quality of management information in relation to incidents that have been escalated to the Health and Safety Executive as RIDDOR reports by the Corporate Health and Safety team has also been identified and is included as an advisory finding (finding 4).

Further information on the findings raised is included at Section 3.

Management Awareness

Education and Children's Services management is aware that improvement is required in this area, and had already made some positive progress with their responses to the EIS and Unison employee unions 'Violence at Work' survey completed in 29 October 2018 and a subsequent elected member motion on 11 December 2018 were detailed in a report presented to the Education, Children and Families Committee in May 2019.

A further survey was completed in December 2019 and a further progress report is due to be presented to the Committee in August 2021 in response to this survey. It is important to ensure that this includes details of the agreed actions that will be implemented in response to the findings raised in this report.

Covid-19 Impacts

It is also important to acknowledge that during the period of our review (April to December 2020) educational establishments were managing the significant challenges associated with the Covid-19 pandemic which has undoubtedly impacted their capacity and ability to address the findings detailed in this report.

We noted through our engagement with the schools that supported this review that they were working tirelessly to help and protect both pupils and employees, and provide support for the children of key workers throughout the pandemic.

Management Response

Following on from this issue in relation to behaviours of concern being highlighted at the Education, Children and Families Committee, a Management / Trade Union working group was established to address the issue that reports of problematic physical behaviours were not being passed on through the appropriate channels. A campaign to raise awareness was launched, including

- Sharing the revised inclusion policy (Included, Engaged, Involved Part 1)
- Sharpening the process for reporting and following up incidents (for example counselling)
- Promotion and communication

As a result of this work, increases in referrals have been noted, however we are aware that some schools may still not be reporting accurately. The measures we propose will triangulate the data by asking teachers, managers and central staff to regularly compare findings.

Although the Internal Audit sample size was very small, we accept that most schools may need further support to fully embed the procedures and processes that were set out pre-COVID.

3. Detailed findings

1. Policies, Procedures and Complaints	High

1. **Policies –** review of Council and Education and Children's Services (formerly Communities and Families) policies that cover behaviours of concern (BoC) established that:
   - The Council Violence at Work policy was last updated in 2014 and is currently being refreshed by the Corporate Health and Safety and Human Resources teams. The policy is supported by a toolkit that was last refreshed in 2015.
   - There is currently no comprehensive Education and Children's Services policy document, guidance or procedure note to support educational employees on managing BOC incidents in educational establishments.

     Management has referenced the Included, Engaged and Involved in Edinburgh policy. This policy outlines the City of Edinburgh approach to inclusion. Appendix One of the procedure lists all of the associated documents including the Relationships, Learning and Behaviour Procedure which includes specific reference to managing BoC when they occur, in terms of recording and Reporting Physical Incidents and Near Misses (Section 19) and Support to Staff and Debriefing (Section 20).
   - Education and Children's Services Procedures and flowcharts that provide guidance on managing BoC incidents are included in the Business Manager's Toolkit / Inclusion Hub. However, Business Managers (BMs) have advised that these tools are not consistently used, and that there is currently no notification issued through the toolkit to advise that documents have been added or refreshed.
   - Some schools have established their own BoC procedures.
2. **Application of Procedures** - review of application of Education and Children's Services BoC procedures across four schools highlighted that they are not consistently applied. Specifically:

   <u>Relationships, Learning and Behaviour procedure</u>

- Verbal debriefs are held following BoC incidents and these are not documented. The procedure requires a documented briefing note that is then shared with concerned stakeholders.
- As incident debriefs are not documented, it is not possible to identify lessons learned and feed these into child planning; risk management planning; and whole school strategic work on predictable needs as detailed in the procedure.
- Pastoral notes on the SEEMIS education management information system are not consistently updated with details relevant to the care and planning of individual pupils due to capacity challenges. Head Teachers confirmed that these details are duplicated with the information also recorded on the SHE Assurance Portal.
- As incident debriefs are not documented, it was not possible to confirm whether impacted employees had been offered counselling and support as detailed in the procedure and 'violent incident reporting flowchart'.

Managing and Reducing Risk procedure

- Review of risk assessments / child plans in a sample of schools highlighted that the forms used are not consistent with the Risk Assessment and Management Plan template.
- Forms are not consistently updated following an incident, and Head Teachers advised that forms are only updated when changes to risk assessments and child plans are required.
- Forms are not supported by version control.

Health and Safety - Incident Reporting – review of incidents reporting through Council's SHE Assurance Portal highlighted that:

- Understanding of the incident record keeping requirements is inconsistent. One school confirmed that they do not retain hard copies of the Incident Reporting Forms to comply with the Council's objectives to become paperless.

  A Corporate Health and Safety advisor confirmed that these hard copy forms should be retained to support potential RIDDOR investigations and to address concerns around the consistency of information reported on the submitted incident forms and information recorded on SHE system.
- One school has recorded the incidents on Behaviour Tracking forms rather than Incident Forms.
- 80% of incidents reviewed were not reported within the 2-day requirement. Head Teachers confirmed that they cannot consistently meet the 2-day deadline for incident recording.
- Schools did not fully understand the importance of accurately recording incidents in the SHE Assurance Portal, which is used by the Corporate Health and Safety team to identify any incidents that should be reported to the Health and Safety Executive (HSE). Schools also advised that once an incident was reported, no further feedback was received.

3. **Complaints and Escalation Process**

   There is no established Education and Children's Services complaints and escalation process that enables employees to complain or escalate instances where they are unhappy with the incident management.

   Discussions with management and employees confirmed that teachers would normally raise complaints with their Union representatives, and Support Staff would raise a grievance through the Councils established grievance procedure.

Management also advised that where significant incidents (for example incidents resulting in employee injury) occur, Head Teachers would contact either a Quality Improvement Education Officer (QIEO) or the Senior Education Manager to advise via phone call or e mail.

Risk

The potential risks associated with our findings are:

- Council and Education and Children's Services policies and procedures that cover behaviours of concern (BoC) are not aligned with applicable legislative and regulatory requirements.
- Potential legislative and regulatory breaches if policies and procedures are not consistently applied.
- Lessons learned are not identified; communicated; and incorporated into future practice.
- Risk assessment and child plans are not consistently reviewed updated (where required) to reflect incident outcomes and lessons learned.
- Counselling or other post incident support is not consistently offered to employees.
- Incidents are not consistently recorded on SHE or are not recorded within applicable timeframes.
- Complaints in relation to handling BoC incidents are not consistently recorded and managed, and significant incidents are not consistently escalated.

1.1 Recommendation: Policy and Procedures (H&S)

1. Human Resources has already commenced a refresh of the policy, and with will be completed with support from the Corporate Health and Safety team.
2. Following review the Policy will be incorporated into a suite of Corporate Health and Safety policies aimed at responding to legislative requirements and recognised workplace hazards, including concerning behaviours.
3. Following this transfer, the policy will either be reviewed as part of the ongoing policy review process that is currently being established by Corporate Health and Safety or in line with any material changes in relevant legislation or regulations.
4. Following the refresh of the current policy Human Resources will arrange for its inclusion in the Council's policy register; publication on the Orb; and communication across all Council directorates; divisions; and services

1.1 Agreed Management Action: Policy and Procedures (Human Resources)

1. The Human Resources Division has already commenced a refresh of the policy, that will be completed with support from the Corporate Health and Safety team.
2. Following review the Policy will be incorporated into a suite of Corporate Health and Safety policies aimed at responding to legislative requirements and recognised workplace hazards, including concerning behaviours.
3. Following this transfer, the policy will either be reviewed in line with the review process that is being established by Corporate Health and Safety, or in line with any changes in relevant legislation or regulations.
4. Following the refresh of the current policy Human Resources will arrange for its inclusion in the Council's policy register; publication on the Orb; and communication across all Council directorates; divisions; and services

Owner: Stephen Moir, Executive Director of Corporate Services, **Contributors:** Nick Smith, Service Director: Legal and Assurance, Chris Lawson, Head of Health and Safety, Katy Miller; Service Director: Human	**Implementation Date:** 28 February 2023

Resources; Martin Young, Head of Employee Relations, Policy and Reward; Layla Smith, Operations Manager, Corporate Services; Michelle Vanhegan, Executive Assistant.	

1.2 Recommendation: Policy and Procedures (Education and Children's Services)

1. Following revision of the Council's Violence at Work policy, Education and Children's Services should complete a comprehensive review of relevant policies and procedures to confirm that they are aligned with Council policy requirements. This should include consideration of whether centralised comprehensive guidance should be prepared and applied across all educational establishments.

   The refreshed procedures should include (but should not be limited) to guidance that addresses the points noted in the finding above, including guidance on the requirements to update risk assessments and pupil plans, and the need to report all incidents via the SHE Assurance Portal.
2. Ownership of policies and procedures should be appropriately allocated, and review dates set that align with any refreshes of the Council's Violence at Work policy.
3. The refreshed policies and procedures should be communicated to all schools with a clear expectation that they should be consistently applied to all violent and aggressive behaviour (BOC) incidents.
4. The refreshed policies and procedures should be published on the Business Manager's Toolkit and the Inclusion Hub.

1.2 Agreed Management Action: Policy and Procedures (Education and Children's Services)

A very comprehensive suite of guidance is currently in place through the Included, Engaged and Involved Policy and associated procedures. This includes the management of behaviours of concern, which covers proactive planning for prevention and also management and recording of these behaviours.

Ownership of policies and procedures and review dates are indicated on the front page of each policy and procedure, and updated information about record retention has been shared with Business Managers.

Further actions to address the points raised by Internal Audit include nominating a lead officer for Managing Behaviours of Concern (Policy and Practice). Their responsibilities will include:

1. Reviewing / cross referencing all relevant procedures with revised Council and Scottish Government guidance;
2. Highlighting revisions to the policies and procedures and share with Headteachers and Business Managers via the Inclusion Hub and School Business Manager Toolkit.
3. Setting annual calendar and version controls
4. More explicitly incorporating the flow charts and procedures for managing problematic behaviour in educational settings
5. Adding this suite of documents to the Inclusion Hub and School Business Managers' Toolkit
6. Calling quarterly meetings with school Assisted Support for Learning team leaders and Health and Safety Committees to review behaviours of concern statistics and lessons learned
7. To report details of statistical outcomes and lessons learned at Education, Children and Families Committee annually

Owner: Julien Kramer, Interim Executive Director of Education and Children's Services, **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of	**Implementation Date:** 30 September 2022

Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	

1.3 Recommendation: Quality Assurance

1. An ongoing risk-based quality assurance process should be designed and implemented to confirm that schools are consistently applying relevant behaviours of concern processes and procedures.
2. The outcomes of this quality assurance process should be reported to senior management and relevant governance forums.

1.3 Agreed Management Action: Quality Assurance

This is usually covered as part of Supported Self-Evaluation / Validated Self-Evaluation visits undertaken in a sample of schools in the course of a school year. Good practice and concerns are communicated to Senior Education and Quality Improvement Managers as appropriate and improvement actions identified. Where there are schools with high levels of incidents as reported on the SHE Portal, this is followed up by the Quality Improvement Education Officer to make sure any specific issues are identified and addressed.

Given that the current restrictions continue to prohibit school visits, this session sampling will be undertaken as a desktop exercise.

Further actions to address the Internal Audit recommendations are as follows:

The Lead Officer for Managing BoC will report quarterly to the Education Management Team to enable discussion with senior education managers on both statistics and lessons learned:

- Following meetings with school Additional Support for Learning team leaders
- Following analysis of incidents included in the SHE portal

Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 June 2022

2. Employee Induction and Training — **High**

Discussion with schools management confirmed that they focus on approaches that should prevent the occurrence of behaviours of concern (BoC) incidents, with the objective of reducing the likelihood of their occurrence.

Review of established Education and Children's Services induction and training arrangements that focus on prevention of; the response to; and subsequent management of BoC incidents confirmed that:

1. **Whole School Autism Training -** there is a lack of clarity in relation to the required frequency for completion of whole school autism training.

   Discussions with Education and Children's Services managers and headteachers confirmed that this should be completed every three years, however the learning and development essential learning spreadsheet for primary, secondary and special schools that advises employees on the

frequency of training to be completed confirms that whole school autism training should be completed 'on employment'.

Additionally, one school advised that whole school autism training was best practice, and not mandatory.

2. **Pupil Support Assistants (PSAs)** who provide support to children (including those with additional learning needs) do not have sufficient time to review policies and complete training as their contracted hours are specifically aligned with school hours, and time focused entirely on when their allocated pupils attend school.

   Additionally, not all PSAs have access to laptops, enabling them to review relevant policies and complete training.

3. **Responding to BoC incidents** - there is no established induction or ongoing training that specifically covers the processes that should be applied in response to BoC incidents and their subsequent management within schools.

4. **Inconsistent induction training content** – the content induction training provided varies across schools and does not include specific reference to relevant BoC policies.

   Review of a sample of induction packs for four schools confirmed that:

   - one school had included the 'Violence at Work' policy folder;
   - one school had included a briefing on 'Accident Prevention and Reporting'; and
   - two schools were unable to provide induction packs.

5. **Employee support** - training does not include information on employee access to support services such as counselling

6. **Training completion -** there is currently no established monitoring mechanism to ensure that all educational employees have completed relevant training. This is particularly relevant for new employees where scheduled whole school training sessions may be (in some cases) circa two to three years after their start date.

   Discussions with head teachers also confirmed that they do not have access to Essential Learning records to confirm completion of training by employees.

Risk

The potential risks associated with our findings are:

- Increased volumes of violent and aggressive behaviour (BOC) if prevention training is not consistently completed by all employees, and pupil support assistants do not have capacity to review policies and complete training.
- BOC incidents are not managed effectively and in line with applicable legislative and regulatory requirements and Council policies when they occur.
- Longer term impacts on employee health and well-being if they are not aware of and do not request support (where required) following BOC incidents.

2.1 Recommendation: Education and Children's Services Training Refresh

1. A centralised approach supporting the development; refresh; delivery; and completion of training across schools should be developed and implemented, with responsibility for this process allocated to an appropriately skilled and experienced employee.
2. Following allocation of responsibilities as per point 1 above, a refresh of Education and Children's Services induction and ongoing training should be performed. This should include (but not be

limited to):

- Developing a consistent induction and ongoing training approach that should be applied and delivered across all schools and educational establishments;
- Specifying the frequency of ongoing training, including whole school autism training;
- Designing and implementing training that focuses on how to manage violent and aggressive behaviour incidents when they occur. This should also include the availability of support for employees following the occurrence of violent and aggressive behaviour (BOC) incidents.
- Specifying the nature and frequency of training to be completed (for example, mandatory training or best practice guidance; and 'on induction', annually, every X number of years).

  This specification should be aligned with the schools and educational establishment's current risk profile and the frequency and nature of incidents that occur, with frequencies increased or decreased as required.

3. A centralised approach to monitoring completion initial induction and ongoing training by employees should also be designed and implemented, with appropriate follow-up performed and action taken where employees are not consistently meeting their training requirements.

2.1 Agreed Management Action: Education and Children's Services Training Refresh

Extensive training on additional support needs, including virtual training and CECiL modules, is currently available. This includes Core Support Staff training to be completed over a three-year period, with training in identified key priority areas completed first.

The Empowered Learning Inclusion Board has a workstream focused on review of existing training for working with learners with additional support needs. Updated information to clarify the frequency of training and which training is mandatory will be shared with schools through this workstream.

The following additional actions will be undertaken to further support this work:

1. The Lead Officer for Managing BoC will link with the Lead Officer (newly qualified teachers / students); Senior Education Officers (with responsibility for training supply staff); and additional support for learning deputy headteachers to deliver training on Included Engaged and Involved for schools employees including: supply staff; newly qualified teachers; and newly appointed staff. This will include managing problematic behaviour, de-escalation and reporting.
2. Headteachers will ensure that Pupil Support Assistants will complete core training within core hours, and this will be reinforced via a briefing note to all Headteachers.
3. Headteachers and Business Managers will ensure online training records maintained and sign off on the Schools Assurance Framework
4. Senior Education Managers will ensure compliance through annual review of the Schools Assurance Framework per locality

Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 June 2022

2.2 Recommendation: Pupil Support Assistants

1. Pupil Support Assistant (PSA) contractual arrangements should be reviewed to ensure that they have sufficient time to complete their initial induction and ongoing training requirements.
2. Arrangements should be established to ensure that PSAs can access the Learning and Teaching Network and relevant network drives and systems (for example the Inclusion Hub) to enable completion of training.

2.2 Agreed Management Action: Pupil Support Assistants

To ensure that all Pupil Support Assistants are able to access essential training schools we would expect schools to make arrangements for this to be done on in-service days and/or other agreed times during the working week.

We believe that all school staff have access to the intranet and relevant network drives and systems. To confirm this and to allow us to identify any issues with this, we will also undertake the following actions:

Where Headteachers report barriers to staff accessing training, including access to devices, they will be supported by their Assisted Support for Learning team leader and Educational Psychologist in the first instance to ensure that Pupil Support Assistants have access to relevant technology equipment and complete core training whether online or in-person within core hours.

Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 June 2022

3. Governance and Management Information — **Medium**

Review of Education and Children's Services governance arrangements for ongoing management oversight of behaviours of concern (BoC) incidents highlighted that:

- There are no established terms of reference for either the Education and Children's Services (formerly C&F) Risk Committee or the Health and Safety Group that confirms whether they have responsibility for oversight and monitoring of health and safety management information (MI), including BoC incidents.
- It was not possible to confirm from committee minutes and action logs whether BoC incidents are scrutinised at these forums.
- It has not been possible to confirm whether incident MI is shared with Education and Children's Services senior managers to review reported incidents, identify any significant trends and take appropriate actions to prevent recurrence.
- There is limited understanding within Education and Children's Services of how to produce meaningful reports from the SHE Assurance Portal that can be shared with management.
- There is no specific BoC / Physical Incidents risk included in the current Education and Children's Services (formerly C&F) risk register (dated 12.01.21).

Risks

The potential risks associated with our findings are:

- Governance of health and safety incidents (including behaviours of concern (BoC)) is not fully effective.
- Limited oversight of BoC and other health and safety incidents.
- BoC risks are not identified; assessed; and effectively managed.

3.1 Recommendation: Committee Terms of Reference

Terms of reference should be prepared and approved for the Education and Children's Services (formerly C&F) Risk Committee and Health and Safety Group that clearly define:

- the roles and responsibilities of both committees; and
- the level of scrutiny to be performed on health and safety incidents (including violent and aggressive behaviour).

3.1 Agreed Management Action: Committee Terms of Reference

Terms of reference will be refreshed for the Education and Children's Services (formerly C&F) Risk Committee and Health and Safety Group that clearly define:

- the roles and responsibilities of both committees; and
- the level of scrutiny to be performed on health and safety incidents (including problematic behaviour).

Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 September 2021

3.2 Recommendation: Scrutiny from Governance Forums

The minutes from both the Education and Children's Services (formerly C&F) Risk Committee and the Education and Children's Services (formerly C&F) Health and Safety Group should include sufficient detail to confirm that significant and thematic health and safety (including behaviours of concern behaviour (BoC) incidents) have been reviewed and considered with appropriate actions agreed and allocated (where appropriate).

3.2 Agreed Management Action: Governance Forums Effective Monitoring

Annual report will be prepared by the Lead Officer for Managing Behaviours of Concern (BoC) detailing

- training
- statistics
- analysis & lessons learned
- next steps

Additionally, the Lead Officer for Managing BoC will either attend the quarterly Education and Children's Service Risk Committee or provide some input on trends to support their ongoing assessment of this risk.

Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 June 2022
3.3 Recommendation: SHE Assurance Portal Training	
Education and Children's Services should request provision of training from the Corporate Health and Safety team on how to extract meaningful incident reports from the SHE Assurance Portal.	
3.3 Agreed Management Action: SHE Assurance Portal Training	
The Corporate Health and Safety team are currently updating SHE training to provide information about the revisions to the portal, the new SHE app and how to extract meaningful reports. Further agreed actions are: This will be shared with headteachers; Business Managers and Quality Improvement and Education Officers; Quality Improvement Managers; Senior Education Managers at the start of the new session.	
Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 September 2021
3.4 Recommendation: Sharing Health and Safety Management Information	
Incident reports extracted from the SHE Assurance Portal should be shared with Education and Children's Services senior managers highlighting thematic trends and recommending actions / lessons learned to prevent recurring incidents.	
3.4 Agreed Management Action: Sharing Health and Safety Management Information	
Incident reports have been requested for discussion at Education Management Team meetings. This would be covered as part of actions 1.3 and 3.2 above.	
Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 June 2022
3.5 Recommendation: Education and Children's Services Risk Register	

1. A specific risk relating to Behaviours of Concern / Physical Incidents should be recorded and assessed in the Education and Children's Services risk register.
2. The current risk rating should be reassessed in line with the volume of incidents experienced.

3.5 Agreed Management Action: Education and Children's Services Risk Register

Risk Register will be updated to reflect ongoing work

The volume of referrals should be seen as positive as this was the aim of the campaign in 2019/20. Analysis will be undertaken to establish the severity of the incidents reported.

This will be discussed at Education Management Team meeting in September

Owner: Julien Kramer, Interim Executive Director of Education and Children's Services **Contributors:** Lorna French, Acting Head of Schools and Lifelong Learning; Gillian Barclay, Depute Principal Psychologist; Kirsty Spence, ASL Head of Inclusion Supports, Anna Gray, Quality Improvement Manager for Special Schools and ASLS; Lynn Paterson, Senior Education Manager; Michelle McMillian, Operations Manager.	**Implementation Date:** 30 Sept 2021

4. Health and Safety – Incidents reported to the Health and Safety Executive	**Advisory**

Review of the SHE incident reporting process highlighted that there is no system field that records whether incidents have met RIDDOR reporting requirements and were subsequently reported to the Health and Safety Executive as RIDDOR records are maintained separately from incident forms

It is acknowledged that there is no regulatory requirement to record this information, however this could provide beneficial management information for directorates in relation to the significance of their incidents.

The Corporate Health and Safety team has confirmed that advisors may note RIDDOR reporting in the system comments section for each incident, and that full incident reports are created and available on request.

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation of the Council which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation of the Council.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation of the Council.
Low	A finding that could have a: • ***Minor*** impact on operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the Council.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Appendix 2: Areas of audit focus

The areas of audit focus and related control objectives included in the review are:

Audit Area	Control Objectives
Governance	• Management Information has been established to enable oversight of recorded concerning behaviour incidents and these are reported to the appropriate governance forum. • Appropriate governance forums with clear terms of reference and reporting structures have been established with responsibility for management oversight of concerning behaviour incidents. These governance forums review reported incidents, identify any significant trends and take appropriate actions to address recurring incidents. • Behaviours of concern risks are included in the directorate risk register with mitigating actions and residual risk regularly updated. • Details of new approaches and proposed process changes and improvements designed to prevent and manage concerning behaviours are regularly reported to the Education, Children and Families Committee, as requested, for scrutiny and oversight. • There is regular liaison with Educational employee Trade Union members to receive their concerns and suggestions and communicate the progress on steps taken to address significant and recurring violent and aggressive incidents.
Policy and Procedures	• The Council has established clear policies, procedures, and guidance that is aligned with applicable legislation to identify, record, report, and manage concerning behaviour incidents in educational establishments. • Procedures and guidance clearly define roles and responsibilities for both teaching and support employees to report and manage/address the incidents. • Policies and procedures include details of the process to be applied for teaching, and support employees who are unhappy with the actions taken to address incidents and prevent their recurrence. • Policies, procedures and guidance have been clearly communicated to all educational employees and can be easily accessed for reference by them in hard copy at school premises and over the organisational intranet. • The induction pack for teaching and support employees in includes information on the arrangements established in their respective schools to manage concerning behaviours, that is aligned to the Council's managing violent and aggressive behaviour policies, procedures and guidance. • Procedures have been established to ensure that teaching and support employees are aware of the pupils in their schools with additional support for learning (ASL) needs and their expected behaviours, and those pupils who have demonstrated concerning behaviours in the past. • Every pupil with ASL needs has an appropriate plan which details the approach to be taken to help them achieve specified learning outcomes and help mitigate the risk of dysregulated behaviour. These plans are made available to all teaching employees.

Audit Area	Control Objectives
Training	• Training has been designed and delivered to teaching and support employees to ensure they aware of the Council's established policies and procedures; are adequately equipped to perform risk assessments; can implement appropriate measures to potentially prevent occurrence of behaviours of concern; and manage incidents when they happen, including incident reporting on the SHE system. • An effective monitoring mechanism is in place to ensure that all educational employees have completed the relevant training. • Employees are made aware of the support services available (for example, occupational health support) concerning behaviour incidents.
Incident Reporting	• All behaviours of concern incidents are accurately and consistently recorded on the SHE system by appropriate managers and appropriately classified by Corporate Health and Safety department as per applicable HSE requirements. This should include, but not be restricted to, the cause of the incident; its significance; actions implemented to manage the incident; and the final outcome. • There is clear evidence to show that suitable responses and support, addressing all the concerns with actions taken for improvement, have been provided to employees involved in incidents. • A reporting mechanism is in place to ensure that all reportable incidents are reported to HSE in accordance with Health and Safety legislative requirements.
Complaints	• Incidents escalated, or complaints raised by staff members are suitably recorded and allocated to an independent investigator. • An escalation process is in place to ensure that all serious concerns are escalated to Head of Service/Executive Director for further investigation. • Once investigations are complete, feedback is provided to the complainant. • Key lessons learned are used to inform and update policy and procedures.

The City of Edinburgh Council
Internal Audit

COVID-19

Spaces for People Programme

Final Report

16 July 2021

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.

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Covid-19 007

Spaces for People Programme

Findings Raised: 0 | 2 | 1 | 0

Background

In response to the Covid-19 pandemic, the Scottish Government (SG) implemented lockdown measures in March 2020, requesting citizens to stay at home (where possible) and maintain a physical distance of at least 2 meters from anyone who does not live in the same household.

The SG strategic framework was published in October 2020 and details the government's current approach to managing the virus. The framework includes five different protection levels that can be applied across local authority geographies, depending on the rate of infection in each area. Each framework level includes different requirements (for example closure of all non essential shops under tier four restrictions, and the requirement not to travel unnecessarily between areas in different tiers) that will directly impact the traffic and footfall in different geographical areas.

To support the government's framework approach and ensure that public health risks associated with Covid-19 are effectively managed, it is essential that adequate space is provided across city, enabling citizens to move around freely and safely whilst adhering to social distancing requirements.

The Council's Spaces for People (SfP) programme was implemented in response to Covid-19 with the objective of implementing a range of temporary changes to streets, pavements and pathways using Temporary Traffic Regulation Orders (TTROs) enabling citizens to safely walk; cycle; and wheel for essential travel and exercise during the pandemic.

SfP implementation timeframes were challenging. Consequently, initial projects for considered for implementation was based on suggestions from a small group of officers and stakeholders, and were implemented under the Council's emergency decision making arrangements implemented in response to Covid-19.

Use of TTROs is regulated by section 14 (1) of the Road Traffic Regulation (RTRA) Act 1984 that enables local authorities to implement temporary measures in certain circumstances (including instances where public safety is at risk) that can remain in place for up to 18 months for roads or carriageways, or 6 months for footpaths or cycleways.

The SfP programme was funded by an initial tranche of £5m funding secured from SUSTRANS, a UK walking and cycling charity, as part of their Spaces for People temporary infrastructure programme which is open to statutory authorities.

Scope and approach

Scope

Our objective was to assess the design of processes implemented to support prioritisation and implementation of SfP initiatives.

We also considered whether the following key risks had been considered when designing the processes supporting the SfP programme, and whether process controls adequately mitigate these risks in line with management's risk appetite:

- Financial risk – demand for changes to public spaces across the city exceeds available funding
- Reputational Risk – limited public consultation and/or high risk priority areas are not identified in a timely manner
- Public Health risk – changes implemented do not support safe movement of citizens across the city in line with Scottish Government social distancing requirements
- Governance and decision making risk – requests are not appropriately prioritised for approval; decisions are not referred to an appropriate level of management / relevant committee; and rationale supporting decisions are not recorded.
- Resourcing risk- insufficient workforce capacity to support implementation of approved changes across the city
- Procurement risk – inability to procure external contractors to support completion of works where internal workforce capacity is insufficient

Approach

1. Discussions with management to understand their appetite in relation to the risks noted above;
2. Performing walkthroughs of the end to end process to identify and understand the design of key process controls;
3. Assessing whether the key controls were adequately designed to mitigate the key risks and were aligned with risk appetite; and
4. Identifying areas where the design of the controls required improvement.

Opinion

Completion Date

Audit work was completed by 10 October 2020 and our opinion and findings are based on the progress of he SfP Programme as at that date

Opinion

Whilst recognising the challenges associated within urgent implementation of SfP initiatives to support citizens during initial Covid-19 lockdown measures, our review identified some significant and moderate control weaknesses in both the design and documentation of controls established to support identification and prioritisation of SfP proposals; project management and governance; and financial and budget management.

Consequently one High and two Medium rated findings have been raised reflecting the need to ensure that the proposal prioritisation process is clearly defined and documented; models used to support proposal prioritisation and financial management are validated; initiative implementation progress and benefits monitoring processes are implemented; appropriate arrangements established to support ongoing public surveys and implementation of feedback (where appropriate) into the design of SfP proposals; and a process established to calculate programme exit costs and determine how these will be funded

Management had identified a number of areas where improvement was required, and had either addressed them (for example, retrospective publication of prioritisation outcomes) or were implementing improvements (for example, creating a programme risk register) during the audit or as at our audit completion date.

Management has advised that additional funding has been requested from Sustrans to support future SfP initiatives, and it will be important to ensure that our audit recommendations are addressed to support their implementation.

Areas of good practice

- All programme proposals were approved by the Council's Incident Management Team (CIMT);
- Public survey feedback resulted in inclusion of additional proposals, and budget reserved to support their implementation.

Spaces for People Programme – management response

Spaces for People (SfP) was established specifically in response to the outbreak of Coronavirus (COVID-19). The purpose was to provide increased space for people to move around safely whether walking, cycling or wheeling. In this emergency situation, the arrangements for introducing the Spaces for People programme could not achieve the normal programme governance arrangements for road and transport schemes therefore an amended approach was developed to recognise the emergency situation and to introduce measures which would have an immediate impact of the public.

Finding 1 - Prioritisation and Approval of Spaces for People (SfP) Initiatives

The first recommendation suggests taking action on the programme to retrospectively review all of the schemes which have been implemented since May 2020. Given the pressures on the project team, it is not proposed to progress this beyond the actions which have already been taken (as set out below).

The initial schemes proposed for inclusion in the programme were approved by Policy and Sustainability Committee on 14 May 2020 under emergency powers alongside the prioritisation scoring matrix and a dedicated notification process, reflecting that public engagement was not feasible for each scheme given urgency required for implementation. All schemes were subject to notification to Local Ward Councillors, Police Scotland, other Emergency Services and key stakeholders. All feedback was considered and scheme proposals were updated (if appropriate) before being considered by the SfP Board and then by the Council's Incident Management Team before discussion with the Council Leader and Depute Leader, prior to implementation of the schemes. Where necessary, Temporary Traffic Regulation Orders were put in place.

Moderation of the scheme prioritisation process in April/May 2020 was undertaken by two experienced members of the Council's Active Travel team. This recognised both the speed of decision making/implementation required, ensured a consistency of approach and provided cover for absence.

The Policy and Sustainability Committee was regularly updated on the schemes which had been implemented and those proposed, with reports provided on: 11 June 2020; 23 July 2020; 20 August 2020. The August report also included further details on prioritisation/scoring matrix.

The public survey was designed to be a forward looking gap analysis with the objective of obtaining public views on what other potential spaces for people initiatives could be implemented From July 2020, Commonplace feedback was incorporated into the Scheme proposals which were submitted to CIMT for approval and instructions were issued to the design team to enable them to access the Commonplace feedback and to take this into account when designing/refining schemes. A summary of the feedback received through Commonplace was presented to Policy and Sustainability Committee in August 2020 and on 12 November 2020 details of how the Commonplace feedback related to the existing schemes was provided. This report also included recommendations additional schemes suggested through the Commonplace survey would were incorporated into the wider programme.

Since completion of the audit, all schemes are reviewed on a two monthly basis, with recommendations for changes reported to Committee for approval. Where relevant, survey outcomes (including negative feedback) was shared with scheme designers at the design review group.

The second recommendation focused on future SfP initiatives. While SfP was a scheme developed specifically in response to Coronavirus (COVID-19) and therefore no further initiatives are expected, in developing proposals to potentially retain some of the existing SfP measures to support the Council's wider priorities for active travel, this recommendation has been considered.

Finding 2 – Project Management and Governance

The SfP programme has now been fully implemented. Improvements to the project management and governance arrangements were implemented following the audit, taking account of the feedback received where possible. In respect of Commonplace, the data relevant to Edinburgh has been downloaded from the system and therefore system access is no longer required.

Finding 3 – Financial and Budget Management

Financial planning meetings have been undertaken every week with an Accountant from the Finance team and the SfP Project Manager. The financial position was reported to Committee, with the scheme reviews, every two months. Following the audit, a budget was set aside in the overall removal of schemes when they are no longer required. This was reviewed regularly and updated if considered necessary.

The schemes implemented were developed and introduced in response to COVID-19, to enable safe physical distancing and to create space for people walking, cycling and wheeling. As noted above, following completion of the audit, each scheme was reviewed every two months and recommendations made for continuing, amending or removing measures.

Arrangements for the potential future retention of schemes was reported to Transport and Environment Committee and then to Council in June 2021.

These high level management comments are supported by more detailed comments on pages 4 – 6 below.

1. Prioritisation and Approval of Spaces for People (SfP) Initiatives

Observations

Whilst it is acknowledged that programme implementation timelines were challenging with circa 100 project proposals to be assessed and prioritised for urgent implementation, and that limited data was available to support the process, the following areas for improvements in the SfP prioritisation and approval process have been identified:

1. **Initial Proposals** - initial SfP initiatives considered for prioritisation were based on suggestions from a relatively small group of officers and external local community stakeholders. Management has advised that subsequent comparison between the programme and retrospective public consultation outcomes demonstrated a good degree of alignment.
2. **Prioritisation Process** – given prohibitive implementation timeframes, the majority of initiatives were initially prioritised by six project team members in April 2020 using the 16 approved scoring criteria in the Prioritisation and Assessment Scheme Model (PASM) spreadsheet. Review of the model methodology and project team assessment approach confirmed that they were largely based on professional judgement with limited justification available to support prioritisation outcomes other than the numeric scores generated by the model.
3. **Prioritisation Guidance** – use of a simple impact matrix supported by verbal team briefings on how the PASM spreadsheet should be used by the project team resulted in inconsistent prioritisation outcomes.
4. **Outcome Review and Moderation -** initial prioritisation outcomes were reviewed and moderated by two project team members using their professional judgement. Whilst different versions of the PASM spreadsheet outcomes were retained, there is no clear audit trail supporting the changes made. Consequently, final prioritisation decisions were based mainly on the professional knowledge and judgment of two project team members.
5. **Outcome Publication** - prioritisation outcomes (scoring and prioritisation ratings) could not be easily located on the Council website, and were not shared with stakeholders prior to approval by CIMT and subsequent implementation.
6. **Public Survey** - public opinion was obtained from a survey completed in June 2020 using the Commonplace survey application, with circa 4,000 comments and 30,000 agreements / likes received. Given time taken to analyse responses, the full population of responses received had not been cross referenced to ongoing SfP initiatives and incorporated (where appropriate) into the prioritisation process prior to completion of the audit (October 2020). It is acknowledged that work was in progress to summarise key themes and map them against initiatives for subsequent Transport and Economy Committee paper.
7. **Use of Feedback** - where public feedback was incorporated into projects, no audit trail was available to confirm that this was completed.

Recommendations

1. Management should consider implementing the following retrospective actions in relation to the most significant and challenging SfP initiatives that are either in progress, or have been completed:
   - ensure that prioritisation outcomes and supporting rationale are clearly documented.
   - publish the outcomes of the retrospective prioritisation process.
   - Consider whether any changes to either completed or initiatives in progress are required based on public feedback.
2. To support effective prioritisation and approval of any future SfP initiatives, management should design and implement a process to support assessment and prioritisation of future proposals. This should include, but not be limited to:
   - details of how the PASM spreadsheet scoring criteria works in practice;
   - how the PASM should be used to support assessment;
   - the change management and ongoing version control process to be applied to the PASM;
   - the need to align proposals with public feedback and opinion (where possible);
   - the requirement to document the rationale for any prioritisation recommendations that are either aligned with model outcomes or are subjective and should be considered;
   - documentation to be retained; and
   - the final moderation and approval process

Risks

The potential risks associated with our findings are:

- Governance and decision making risk – proposals are not appropriately prioritised for approval; and the rationale supporting decisions is not recorded.
- Resourcing risk – key person dependency on two project team members to ensure consistency in both the completed and future initiative prioritisation process.
- Reputational Risk – public perception that feedback provided through the Commonplace survey was not considered in relation to ongoing schemes.

Management Comments

The Spaces for People programme was launched by the Scottish Government in April 2020 in response to the Coronavirus (COVID-19) pandemic and the need to provide additional space to support physical distancing when moving around the city, Council officers identified that there were areas where this could be addressed. The programme was developed with prioritisation criteria (based on the guidance available and the timescales for developing and implementing schemes in an emergency situation) and presented to Policy and Sustainability Committee on 14 May 2020. Thereafter monthly programme updates were provided. A scoring matrix for the prioritisation was retrospectively developed and reported to Committee on 20 August 2020.

The framework used for prioritisation was developed by the most experienced members of the team and and, given that the prioritisation was subjective, they carried out a moderation exercise to ensure consistency.

The invitation for residents to identify areas where physical distancing was difficult in the city ran from 29 May to 29 June 2020, using the Commonplace online tool. It was clear that it would not be possible to fulfil every request but that resources would be directed to where they were most needed. In addition to setting aside funding for new measures based on the feedback received, the feedback received was overlaid with the map of existing schemes. Where schemes were still being developed, the feedback was considered as part of the design and reported to CIMT. From October 2020, for existing schemes, the design team were encouraged to take account of feedback received in reviewing scheme designs (the outcome of which was reported to Transport and Environment Committee).

2. Project Management and Governance

Observations

As the SfP programme was initiated at extremely short notice with the majority of initial decisions made under considerable time pressure, a number of routine project management and governance arrangements were either not implemented, or were implemented retrospectively. Specifically:

1. **Project business case** - no business case was developed for the programme. This appears reasonable given tight implementation timeframes.
2. **Project governance** – whilst regular project team and Board meetings are held, outcomes of discussions and decisions are not being consistently recorded. Action logs have been created, but do not consistently include details of action owners. Additionally, progress with delivery of actions is not always monitored at subsequent meetings.
3. **Risk management** - risk appetite for the programme was not clearly defined, and no risk management process was implemented to support identification; assessment; and management of programme delivery risks. It is acknowledged that a risk register has now been established and is currently being populated, and that the health and safety aspects of designs were considered by the design review group.
4. **Initiative implementation and benefits realisation –** due to capacity constraints, no monitoring is performed to confirm that works have been completed in line with specified delivery milestones. Additionally, no assessment has been performed to confirm that expected benefits have been realised. Management has confirmed that peer reviews have been performed following completion of our audit work to confirm the whether expected benefits have been realised.
5. **Commonplace survey tool -** the survey application was sourced on an initial free six month trial period, and it is currently unclear how the Council's SfP survey data will be accessed if the licence is not extended. Additionally, data controller responsibilities have not been clarified between the Council and the application provider in the event that any personal data is collected as part of the survey process.

Recommendations

To support ongoing implementation of SfP initiatives, management should design and implement relevant and proportionate improvements to the established governance and risk management framework. This should include, but not be limited to:

1. documentation of decisions made at project team meetings, including consideration of relevant risks
2. continue to develop and use the programme risk register to support identification; assessment; and effective management of programme risks
3. Identify key project team members and design and implement appropriate processes to monitor ongoing programme delivery in comparison to delivery milestones, and assess whether expected benefits are being achieved.
4. confirm whether the commonplace survey tool contract will be extended, and establish data controller responsibilities in the event that the application is used to collect personal data.
5. If the commonplace contract is not extended, identify and implement alternative arrangements to collect public feedback on SfP initiatives.

Risks

The potential risks associated with our findings are

- Governance and decision making risk – rationale and risks associated with decisions are not recorded; and programme risks are not identified; assessed; and addressed.
- Governance and decision making risk – project delivery timeframes are not achieved and anticipated benefits are not realised.
- Governance and decision making risk – SfP survey data cannot be accessed and data processing roles, responsibilities; and processing activities (where personal data is used) are not clearly defined, with potential legal and reputational consequences.

Management Comments

Management Response:

The Spaces for People Programme was promoted and funded by the Scottish Government and was implemented at pace. However, the rationale for the programme was set out in the report to Policy and Sustainability Committee in May 2020.

It is recognised that, while meeting notes have been prepared and action logs created, there have been instances where the actions have not been consistently recorded and/or have not had action owners identified.

Initial risk management focused on the risk to the public from the transmission of COVID-19 and this was recognised in the operational plan and in the risk register which was prepared at the beginning of the programme. However, risks associated with the programme were regularly discussed at the Spaces for People Board and, where actions were agreed, these are recorded in the meeting papers. A programme risk register was created in September 2020.

Since September 2020, scheme reviews have been carried out every two months to confirm that the schemes implemented are effective and that the anticipated benefits are being realised. This has led to some changes to schemes being proposed to Committee for approval.

The Commonplace survey data for the Edinburgh survey was provided by Sustrans to the Council in order for the analysis of comments and suggestions to be completed. Once the report was presented to Committee, there was no further need for City of Edinburgh Council to access the Commonplace system for information. The responsibilities of the data controller rest with Sustrans.

3. Financial and Budget Management

Observations

Review of the financial controls established to support the SfP programme confirmed that:

1. **Financial Assessment Summary Spreadsheet** – there was limited evidence of validation by the project team of the Financial Assessment Summary Traffic Management spreadsheet designed by external consultants and used to cost the initiatives; determine stock levels required; and select suppliers to confirm its completeness and accuracy prior to use.
2. **Programme Exit Costs** - there is currently no clear strategy for determining the potential exit costs associated with reversing individual projects, or transitioning them into permanent solutions, and it is currently unclear how any significant exit costs will be funded.
3. **Benefits Realisation Funding** – Currently £175K (4% of available SfP funds) has been retained to complete a review of programme benefits by an external consultant, with no supporting rationale for this retention value. Management has advised that this budget allocation was defined following detailed engagement with Sustrans, however no evidence has been provided to support this.

Recommendations

To support effective ongoing management of the SfP programme management should

1. Perform a retrospective review of the Financial Assessment Summary Spreadsheet Summary Traffic Management spreadsheet to confirm the completeness and accuracy of model formulae and assumptions, and that there are no significant inaccuracies in forecast and actual project costs.
2. Develop an approach to support calculation of exit costs and how these will be funded.
3. Consider alternative internal options for completion of the planned benefits review and determine the associated costs. This should include consideration of completion of data gathering and benefits assessments on a continuous basis for the duration of individual projects, enabling ongoing modification to support benefits realisation (where required).

Risks

The potential risks associated with our findings are

1. Financial risk – inaccurate financial outputs are produced from spreadsheet models and used as the basis for decision making.
2. Financial risk – funds retained to cover remediation and benefits realisation costs are not sufficient.
3. Reputational risks - negative publicity associated with potential programme overspends

Management Comments

It is recognised that the financial model was not validated prior to use. However, the recording sheet evolved in discussion with the Project team and Finance to include appropriate functions and cost projections. The actual costs are tracked through the Council's financial systems and show that they are in-line with cost projections, which offers confidence in the developed model.

The initial financial modelling for the programme did not define detailed exit costing. However, this was subsequently developed and a budget has been allocated in the overall programme for full removal or reinstatement based on quotes from the installation contractors.

In January 2021 Transport and Environment Committee approved taking forward a consultation on next steps for Spaces for People programme. The outcome of this was reported in June 2021.

Report Rating Definitions

Effective	**Process controls have been adequately designed and provide assurance (if consistently applied) risks will be managed effectively in line with risk appetite, and the Council's objectives achieved.**
Some improvement required	**Whilst some control weaknesses were identified in the design of key process controls, they provide reasonable assurance that risks are being managed in line with risk appetite and that and the Council's objectives should be achieved.**
Significant improvement required	**Significant weaknesses were identified the design of key process controls. Consequently, only limited assurance can be provided that risks are being managed in line with risk appetite and that the Council's objectives should be achieved.**
Inadequate	**The design of key process controls is inadequate, with a number of significant control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.**