Governance, Risk and Best Value Committee

10.00am, Tuesday, 7 May 2019

Internal Audit Quarterly Update Report: 26 November 2018 to 29 March 2019

Item number	8.1
Executive/routine	
Wards	
Council Commitments	

1. Recommendations

1.1 It is recommended that Committee approves the proposals to carry forward three audits into the 2019/20 plan year.

1.2 It is recommended that Committee notes:

1.1.1 the outcomes of the completed audits;

1.1.2 progress with the delivery of the 2018/19 Internal Audit (IA) plan and the carried forward 2017/18 audits;

1.1.3 that reporting performance against IA key performance indicators will start in the new 2019/20 IA plan year; and

1.1.4 key IA priorities and ongoing areas of focus.

Lesley Newdall

Chief Internal Auditor

Legal and Risk Division, Resources Directorate

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

•EDINBVRGH•
THE CITY OF EDINBURGH COUNCIL

Report

Internal Audit Quarterly Update Report: 26 November 2018 to 29 March 2019

2. Executive Summary

2.1 Three audits have been proposed for carry forward into the 2019/20 annual plan year.

2.2 It is expected that all remaining 2018/19 IA reviews will be completed in sufficient time to support the 2018/19 IA annual opinion which is due to be presented to Committee in August 2019. Initial planning for 2019/20 audit reviews has also started.

2.3 Key IA priorities for the next quarter include ongoing focus on completion of the 2018/19 plan and annual IA opinion; delivery of the 2019/20 plan; ongoing follow-up of open findings; recruiting to vacant roles; performing a TeamCentral post-implementation review; implementation of time sheet recording and reporting; and ongoing delivery of training across the Council.

3. Background

3.1 Internal Audit is required to deliver an annual plan of work, which is scoped using a risk-based assessment of the Council's activities. Additional reviews are added to the plan where considered necessary to address any emerging risks and issues identified during the year, subject to approval from the Governance, Risk, and Best Value Committee (GRBV).

3.2 The 2018/19 IA plan approved by GRBV in March 2018 included 50 audits. This was subsequently reduced to 47 audits in November 2018, when the Committee approved the rebased plan. One further audit (Garden Waste) was added to the plan in July 2018, leaving a total of 48 audits to be completed.

3.3 IA progress and copies of completed reports are presented to GRBV quarterly for their review and scrutiny.

3.4 All audits performed for the Lothian Pension Fund (LPF) are subject to separate scrutiny by the Pension Audit Sub-Committee and the Pensions Committee, and are included in this report for completeness.

3.5 Audits performed for the Edinburgh Integration Joint Board (EIJB) are presented to the EIJB Audit and Risk Committee for scrutiny, with any reports that are relevant to the Council subsequently referred to the GRBV Committee.

3.6 Audits performed for the City of Edinburgh Council (the Council) that are relevant to the EIJB will be recommended for referral to the EIJB Audit and Risk Committee by the GRBV Committee.

4. Main report

Carry forward proposal

4.1 It is proposed that the following three audits are carried forward in to the 2019/20 IA annual plan year:

4.1.1 Payroll – the delayed national pay award agreement for local government employees and teachers, which covers a three-year period, including a significant retrospective element to 1 April 2018, has impacted the availability of Payroll staff to directly support the planned review. It has been agreed with both the Executive Director of Resources and Scott Moncrieff (External Audit) that this review should be deferred until May 2019; and

4.1.2 CGI Change Management and CGI Sub Contract Management reviews – CGI and the Council's Digital Services did not have the capacity to support completion of three scheduled reviews prior to the end of the year, owing to capacity being focussed upon major change programme delivery.

Consequently, it has been agreed with the Executive Director of Resources and CGI that these two reviews should be proposed for carry forward into the 2019/20 plan year, with the specialist PwC Certifications and Software Licencing review to be completed by May 2019 to support the IA annual opinion.

2018/19 Plan delivery progress

4.2 A full reconciliation of the 2018/19 IA plan is included at Appendix, 1 and an analysis of progress with delivery of the remaining 46 audits to be completed to support the 2018/19 IA annual opinion is included at Appendix 2.

Of the remaining 46 audits to be completed to support the 2018/19 IA annual opinion, 15 are now complete. Two of these were for the Royal Edinburgh Military Tattoo; and the South East of Scotland Transport Partnership (SEStran) with the remaining 13 reviews completed across the Council.

4.3 The overall IA report rating outcomes associated with the 13 completed Council reviews are:

4.3.1 Significant Enhancements Required – 5;

4.3.2 Generally Adequate – 4; and

4.3.3 Adequate - 4

4.4 A total of 11 audits are at the draft reporting stage, with three of these draft reports already issued to management; and eight reports currently being prepared.

4.5 A further 17 audits are in progress. Two of these are the agile Tram and Enterprise Resource Planning (ERP) programme reviews that will continue through to programme completion, when final reports that include all IA findings raised and presented to the project boards will be prepared.

4.6 A further two audits, the Looked After and Accommodated Children (St Katherine's) and the Building Standards reviews are also included in the 17 reviews in progress. IA is currently working with Communities and Families to align the outcomes of our St Katherine's review with their proposals to further investigate and resolve historic records management issues and are also engaging with the Place Directorate to determine how best to present the outcomes of our follow-up work to support their ongoing discussions with the Scottish Government.

4.7 Of the remaining 12 reviews in progress, ten are expected to complete by May 2019, with dates for delivery of two Edinburgh Integration Joint Board reviews still to be determined.

4.8 A further three reviews are currently in planning. These are:

4.8.1 Health and Safety – Life and Limb Risks (PwC);

4.8.2 EIJB Partnership Infrastructure and Support – Integration Scheme; and

4.8.3 CGI - Certifications and Software Licencing

Internal Audit Key Performance Indicators

4.9 The IA journey map and key performance indicators was approved by both the Corporate Leadership Team (CLT) and the Committee in January 2019 and are designed to support timely and effective delivery of the annual plan. The key performance indicators (KPIs) specify expected delivery timeframes for both the IA team and management at all stages of the audit process.

4.10 Whilst IA has been tracking performance against the KPIs, it is acknowledged that a significant proportion of the plan was delivered in the last quarter. Consequently, it is recommended that reporting against the KPIs is established for all 2019/20 IA reviews and relevant indicators reported quarterly to Committee.

Progress with Internal Audit key priorities

4.11 We have successfully recruited into the post of principal audit manager, which was being covered temporarily by an existing team member, and auditor roles.

4.12 The 2019/20 IA plan was finalised and approved by the Committee in March 2019.

4.13 The PwC co source contract has been extended for one year, in-line with the contract provisions, enabling us to explore potential joint procurement opportunities with other public sector organisations in the future.

Ongoing areas of focus

4.14 Ongoing areas of focus for Internal Audit include:

4.14.1 Completion of the 2018/19 IA plan and annual opinion and delivery of the 2019/20 plan;

4.14.2 Recruitment – a vacancy at senior auditor level has arisen following the substantive promotion of an existing team member into the post of principal audit manager. An auditor vacancy has arisen with the team due to retirement of a team member;

4.14.3 Performing a TeamCentral post-implementation review following launch of the system to support the follow-up process in July 2018;

4.14.4 Implementation of time sheet recording and reporting enabling us to track and report on time spent on audit delivery and follow up activities; and

4.14.5 Training delivery – a training session on 'Risk, Control and the Three Lines of Defence' is scheduled with the CLT and Heads of Service for the end of May. Ongoing quarterly Council wide training has still to be scheduled.

5. Next Steps

5.1 IA will continue to monitor progress with plan delivery.

6. Financial impact

6.1 There are no direct financial impacts arising from this report, although failure to close IA findings raised and address the associated risks in a timely manner may have some inherent financial impact.

7. Stakeholder/Community Impact

7.1 IA findings are raised as a result of control gaps or deficiencies identified during audits. If agreed management actions are not implemented to support closure of Internal Audit findings, the Council will be exposed to the risks set out in the relevant IA reports.

8. Background reading/external references

8.1 None

9. Appendices

Appendix 1	2018/19 IA Annual Plan Reconciliation
Appendix 2	Summary of 2018/19 IA Plan Progress
Appendix 3	Final Report - Compliance with IR35 and Right to Work Requirements

Appendix 4	Final Report - Public Sector Cyber Action Plan for Cyber Resilience
Appendix 5	Final Report - Street Lights and Road Traffic Signals
Appendix 6	Final Report - Validation of Internal Audit Implemented and Sustained Management Actions
Appendix 7	Final Report - Port Facility Security Plan
Appendix 8	Final Report – Developer Contributions
Appendix 9	Final Report – Communities and Families Self Assurance Review

Appendix 1 – 2018/19 IA Annual Plan Reconciliation

Reconciliation		Comments
Total number of reviews in 18/19 IA Plan	**48**	**Approved by GRBV March 2018**
Add - Reviews carried forward from 2017/18	3	Mela; Structures and Flood Prevention; and Fleet Project.
Add - Reviews added in 2018/19	1	Garden Waste.
Less - Reviews removed from the plan	2	City Deal and Resilience were removed from the plan per November 2018 plan rebase.
Less - Reviews carried forward into 2019/20	4	Care Homes carried forward per November 2018 plan rebase. CGI Change Management; CGI Sub Contract Management and Payroll are also now proposed for carry forward into 2019/20.
Total reviews to be delivered to support 2018/19 IA opinion	**46**	**Refer Appendix 2 below for further detail**

Appendix 2 – Summary of 2018/19 IA Plan Progress

Audit Review			
Completed		**Report Rating**	**Presented to Committee**
1.	Transfer of the Management of Development Funding Grant	**Adequate**	August 2018
2.	Garden Waste – Lessons Learned	**Generally Adequate**	January 2019
3.	Carbon Reduction Commitment Scheme	**Adequate**	
4.	The Edinburgh Mela	**Generally Adequate**	
5.	Structures and Flood Prevention	**Adequate**	
6.	Fleet Project	**Significant Enhancements**	
7.	Compliance with IR35 and Right to Work Requirements	**Generally Adequate**	May 2019
8.	Public Sector Cyber Action Plan for Cyber Resilience	**Significant Enhancements**	
9.	Street Lights and Road Traffic Signals	**Generally Adequate**	
10.	Validation of Internal Audit Implemented and Sustained Management Actions	**Significant Enhancements**	
11.	Port Facility Security Plan	**Adequate**	
12.	Developer Contributions	**Significant Enhancements**	
13.	Communities and Families Self Assurance Review	**Significant Enhancements**	
14.	Edinburgh Royal Military Tattoo – Health and Safety	N/A	N/A
15.	SEStran		
Total reports completed		**15**	
Draft Reports Issued to Management		**Expected Completion**	
16.	Quality, Governance, and Regulation	April 2019	
17.	EIJB Governance Structures		
18.	Portfolio Governance Framework		
Total draft reports issued to management		**3**	
Draft Reports Being Prepared			
19.	System Access Rights	May 2019	
20.	Localities Operating Model		
21.	Organisational Change		
22.	Implementation of asset strategy & CAFM		

Audit Review			
Completed		**Report Rating**	**Presented to Committee**
23.	Implementation of FM SLA		
24.	Major Projects – Schools and Customer Transformation		
25.	GDPR Follow-Up		
26.	Public Services Network and Out of Support Technology		
Total reports being prepared		**8**	
Fieldwork			
27.	Edinburgh Tram Extension	Ongoing agile project review	
28.	Enterprise Resource Planning System Implementation		
29.	Looked After and Accommodated Children (St Katherines)	to be determined	
30.	Homelessness	May 2019	
31.	Payments and Charges (Contractor)		
32.	Emergency Prioritisation and Complaints		
33.	Supplier Management Framework and Construction Industry Scheme (Contractor)		
34.	Edinburgh Roads Services (Contractor)		
35.	Waste and Cleansing Services Performance Management Framework		
36.	HMO Licencing		
37.	Building Standards Follow Up	To be determined	
38.	EIJB Integration Scheme		
39.	EIJB Strategic Planning		
40.	Lothian Valuation Joint Board	May 2019	
41.	Lothian Pension Fund – Unlisted Investments (PwC)		
42.	Lothian Pension Fund - Unitisation		
43.	Lothian Pension Fund – Stock Lending		
Total reviews in progress		**17**	
Planning			
44.	Health and Safety – Life and Limb Risks (PwC)	to be determined	
45.	EIJB Partnership Infrastructure and Support – Integration Scheme		
46.	CGI - Certifications and Software Licencing		
Total reviews at planning stage		**3**	

The City of Edinburgh Council

Internal Audit

Compliance with IR35 and Right to Work Requirements

Final Report

15 March 2019

RES1802

•EDINBVRGH•
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018. 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

IR35

In April 2017, HMRC introduced changes to the IR35 working rules for temporary off payroll workers in public authorities. The objective of these changes was to prevent individuals from working as 'disguised employees' through their own limited company, personal service company or partnership whilst saving on income tax and National Insurance (NI). These individuals, though not employed by the Council, may be subject to income tax and NI if they perform work similar to that of a permanent employee. For example, where the worker is under the supervision, direction, and control of the Council.

As a result, the Council now has responsibility to:

- determine whether the off-payroll working rules should apply, both initially and when future engagements are made;
- monitor the duties performed by the worker to ensure they remain reflective of the initial assessment, and reperform the assessment should these change;
- confirm whether the off-payroll working rules should apply to workers supplied via an agency; and
- respond to any written requests from a worker or agency to set out the reasons for the IR35 assessment outcome within 31 days.

The Council has implemented processes to ensure compliance with IR35 working rules. Responsibility for completing the necessary checks and determining the IR35 status of the worker is devolved to Service Areas, with the engaging manager required to complete the assessment using HMRC's online IR35 assessment tool, prior to engaging the worker.

The outcome of the online assessment then determines the Council's responsibilities and how it subsequently makes payments to workers:

- If the assessment confirms that that the worker is 'Employed for Tax Purposes' then the Council, is responsible for deducting PAYE and NI contributions as if they were a Council employee through its payroll system; or
- If the assessment confirms that the worker is outwith IR35 and not Employed for Tax purposes then the Council would pay treat the worker as a supplier, making payment through the purchase ledger. This process is managed by the Commercial & Procurement Services (CPS) Vendor Team and Banking and Payment Services.

Alternatively, where a recruitment agency is used, payment is made via the agency who subsequently recharges the costs to the Council.

HMRC conducts Employer Compliance Reviews which consider the operation of IR35 rules within organisations. HMRC has confirmed that the will only stand by assessment results that are based on accurate source information.

Right to work

The Immigration, Asylum and Nationality Act 2006, places a duty on the Council to prevent illegal working by undertaking checks on all employees' right to work in the UK. The Council may be liable for a civil penalty if they employ someone who does not have a right to work. The penalty can be revoked if the Council can demonstrate that they have performed the prescribed documentation checks to confirm a legal right to work prior to employment.

In line with Home Office requirements, the Council has implemented processes to conduct right to work checks as part of recruitment and selection processes. Recruiting managers must obtain, check and copy original documents, recording the date the check was conducted. They must also carry out further checks for workers with a limited right to work in the UK. Copies of original documents must be retained for not less than two years after the employment has come to an end.

Scope

This review assessed the design and operating effectiveness of the Council's onboarding controls to ensure that all agency workers/contingent labour are IR35 compliant, and that all new employees have a right to work in the UK. The review also considered ongoing controls within Service Areas to ensure that IR35 compliance and right to work status is maintained.

Our audit work concluded on 24 September 2018 and our findings and opinion are based on the outcomes of our testing at that date.

2. Executive summary

Summary of findings raised	
High	IR35 Compliance and oversight framework
Medium	Inclusion of IR35 responsibilities in contracts for agency worker suppliers
Low	Compliance with right to work requirements

Opinion

Our review of controls established to ensure that the Council achieves ongoing compliance with both HMRC IR35 and Home Office Right to Work legislation confirmed that whilst generally adequate controls have been established to ensure Right to Work compliance, some enhancements are required to ensure ongoing compliance with IR35 requirements.

Consequently, 1 High; 1 Medium; and 1 Low rated findings have been raised.

Whilst some controls have been established that ensure compliance with aspects of IR35 legislation; including payroll procedures for deducting income tax and NI due, areas of weakness have been identified in both the design of the Council's IR35 control framework and operating effectiveness of the established controls. These weaknesses have resulted in instances of non-compliance with IR35 legislation, exposing the Council to potential penalties from HMRC, and repayment of historic employee income tax and NI liabilities.

The High rated finding highlights that processes require to be designed and implemented to ensure ongoing compliance with all aspects of IR35, including the requirement to respond to worker requests for assessment outcome details within prescribed timeframes; and initial and ongoing assessment of the employment status of worker groups (for example Daybreak Carers) and partnerships who provide services to the Council.

The High rated finding also reflects the need to ensure that training and guidance is provided to engaging managers to reflect their full range of IR35 responsibilities when engaging temporary workers.

Our Medium rated finding focuses on the need to ensure that contracts with third party recruitment agencies include details of the respective IR35 responsibilities for both the Council and the agencies, and details of the operational process that should be applied by both parties to ensure that the Council has discharged its duty to determine if IR35 working rules apply to temporary workers sourced from agencies.

We confirmed that controls to ensure compliance with Home Office Right to Work requirements are an integral part of the Councils recruitment and selection processes. Detailed procedures have been developed to ensure that appropriate checks are completed for all new employees, and re-performed where current employees have a limited right to work timeframe.

Review of documentation for a sample of employees identified some minor compliance issues relating to validation of documents confirming employee's right to work, and lack of Council wide monitoring to confirm the extent of ongoing compliance, and ensure that breaches are identified, addressed and reported to the Home Office where required. Consequently, a 'Low' rated finding has been raised.

3. Detailed findings

1. IR35 Compliance and Oversight Framework	High

IR35 Framework

Whilst the Council has established operational processes for assessing the employment status of temporary workers, no overall policy and supporting framework has been established that clearly defines IR35 roles and responsibilities across the Council.

Review of IR35 Operational Processes

Review of existing IR35 operational processes also established the following process and training gaps:

1. **Responding to worker requests** – currently no standard letters are issued to notify the worker or agency of the outcome of the initial IR35 assessment; and no process has been implemented to ensure that responses to worker or agency requests for details of IR35 assessment outcomes are issued within the 31 days specified in the legislation. Management has advised that they are not aware of receipt of any outcome requests to date;
2. **Partnerships** – Where a worker provides services through a partnership, an IR35 assessment should be completed should the partnership meet one of the conditions set out in section 61P of the Finance Act 2017. Management has confirmed that they were not aware of the requirement to assess the status of workers who provide services through partnerships. At the time of our audit, there were circa 300 live partnership vendor records, of which CPS has advised circa 107 are classed as small organisations providing services to the Council;
3. **Daybreak Carers** – At the time of our audit fieldwork, no IR35 assessments had been completed for a small group of approximately 40 workers (Daybreak Carers) provided through Shared Lives to the Health and Social Care Partnership (the Partnership) to provide short-term care to adults. These workers are self-employed and are paid as vendors through Oracle.

   Commercial and Procurement Services (CPS) requested copies of completed IR35 assessments, however were advised by the Partnership that Daybreak Carers may be entitled to HMRC's 'Qualifying Care Relief', and that IR35 requirements may not apply.

   CPS requested that the Partnership obtain a formal opinion from HMRC on the employment status of these workers. This had not been received by the conclusion of our audit fieldwork.

   Since the audit, Shared Lives have obtained an opinion from HMRC, however it is on a case specific basis, and for another local authority, therefore Shared Lives have advised they are unable to provide a copy of email from HMRC to evidence this. The position for City of Edinburgh Council therefore remains unconfirmed.

   Management also advised that Daybreak Carer arrangements are longstanding, and are supported by a 'Carer's Agreement' between the Partnership and the worker. Management advised no agreement was held on file for 2 workers sampled, and the 'Carer's Agreement' document had not been reviewed in some time.
4. **Training**– no training is currently provided to engaging managers to advise them of their initial and ongoing IR35 responsibilities.
5. **Orb content** - Locating the IR35 'off-payroll' process on the Orb assumes prior knowledge of IR35 legislation. The Orb content covers basic HMRC requirements for assessing the status of workers,

but does not provide all of the guidance required to ensure full compliance, including the requirement to:

- Monitor the duties, working arrangements, and integration of workers to ensure they remain reflective of the information which informed the assessment; and
- Reperform the IR35 assessment if the role, responsibilities or contract for a temporary worker changes during the period of engagement.

IR35 Compliance Oversight

Additionally, no oversight or monitoring processes have been established to confirm the extent of ongoing IR35 compliance across the Council, and ensure that breaches are identified; resolved and reported to HMRC (when required).

Instances of IR35 Non-Compliance

A total of 159 temporary workers were engaged across the Council between 1 October 2017 and 31 July 2018. We reviewed of a sample of 20 temporary workers engaged and identified the following areas of non-compliance with IR35 requirements:

1. 16 cases where, the HMRC assessment had been completed after the engagement commenced. Engaging managers sampled advised they had not been aware of this requirement until CPS requested a copy of the assessment to create/update the vendor record for payment. For each of these cases, the worker had been assessed as being outwith IR35;
2. 4 cases where a copy of the IR35 assessment and supporting evidence could not be provided by the Service Area; and
3. 1 case where the worker had completed the assessment themselves and forwarded it to the engaging manager

Risks

- Non-compliance with IR35 regulations;
- Lack of visibility of ongoing compliance with IR35 requirements across the Council, and inability to ensure that breaches are identified; escalated; addressed; and reported to HMRC where necessary;
- Inability to provide evidence to HMRC if required; and
- Potential non-compliance penalties and liability for payment of unpaid contributions to HMRC.

1.1 Documenting end to end IR35 processes

The Council should document and consider publishing via the Orb, the full end to end IR35 process, clearly setting out roles and responsibilities across Service Areas. (A process map was created by Internal Audit during the review which could be adapted and expanded for this purpose).

Agreed Management Action

The process map will be adopted, revised and maintained by Commercial and Procurement Services (CPS) with assistance from Human Resources and Payroll to ensure it clearly documents full end to end processes and sets out clear roles and responsibilities across all Service Areas. The process map will be made available on the Orb.

Owner: Stephen Moir, Executive Director of Resources.

Contributors: Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer; Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant

Implementation Date:

30 September 2019

1.2 Responding to written requests within 31 days

A process for responding to written requests from workers regarding the outcome of their IR35 assessment (within 31 day legislative timeframe for response) should be designed and implemented. This could be achieved by requiring engaging managers to issue standard decision letters (sourced from the Orb) to workers following completion of IR35 assessments.

Agreed Management Action

The IR35 processes will be revised to require the engaging manager to issue a standard decision letter to all temporary workers following completion on an IR35 assessment. The revised process and template letters will be made available to engaging managers via the Orb.

Owner: Stephen Moir, Executive Director of Resources.

Contributors: Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant.

Implementation Date:

30 September 2019

1.3 Services provided by Partnerships

A process should be implemented to ensure IR35 assessments are complete all workers who provide services to the Council through a partnership.

In addition, a review of all current partnership records should be performed to identify where the engaging manager should be requested to complete a retrospective IR35 assessment for the worker.

Agreed Management Action

A new vendor form has been introduced which will trigger the requirement for an IR35 assessment to be complete for all small organisations with a headcount less than 10.

Circa 300 existing vendor records will be reviewed, and where required Commercial and Procurement Services (CPS) will request that the engaging manager complete a retrospective IR35 assessment for the worker.

Owner: Stephen Moir, Executive Director of Resources.

Contributors: Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer.

Implementation Date:

30 September 2019

1.4 Employment status of Daybreak Carers

HMRC should be contacted to obtain a formal opinion whether the IR35 / intermediaries' legislation applies to Daybreak Carers providing services to the City of Edinburgh Council. A copy of the opinion confirmation letter should be provided to Commercial and Procurement Services (CPS) and Human Resources so they can update records as required.

Agreed Management Action

The service has written to HMRC to obtain a formal opinion, this will be forwarded to both Commercial and Procurement Services (CPS) and Human Resources once received.

Owner: Judith Proctor, Chief Officer Edinburgh Health and Social Care Partnership. **Contributors:** Tony Duncan, Interim Head of Strategic Planning; Mark Grierson, Disability Support & Strategy Manager; Anne-Marie Donaldson, Local Area Co-ordinator Manager; Craig Russell, Principal Solicitor – Employment.	**Implementation Date:** 31 July 2019

1.5 Daybreak Carer's Agreements

The current Carer's Agreement should be revised to ensure it clearly specifies the employment status of Daybreak Carers, and it complies with the requirements of General Data Protection Regulations (GDPR) in relation to confidentiality and record retention. All current Day Break Carers should be required to sign the revised agreement. The agreement should be reviewed on an annual basis and carers requested to resign where any revisions have been made.

Agreed Management Action

The Carer's Agreement will be revised with assistance from the Council's Legal and Risk service to ensure it complies with all requirements.

All current carers will be asked to sign a revised agreement. The agreement will be revised on an annual basis to take account of any relevant changes.

Owner: Judith Proctor, Chief Officer Edinburgh Health and Social Care Partnership. **Contributors:** Tony Duncan, Interim Head of Strategic Planning; Mark Grierson, Disability Support & Strategy Manager; Anne-Marie Donaldson, Local Area Co-ordinator Manager; Craig Russell, Principal Solicitor – Employment.	**Implementation Date:** 30 September 2019

1.6 Review of all supplier groups

A review all current supplier groups paid via Oracle should be performed to ensure employment status has been confirmed, and appropriate action taken where retrospective IR35 assessments confirm that these workers should have been 'on payroll'.

Agreed Management Action

All current supplier groups have been identified, however new groups may continue to arise as they are processed through feeder systems. A vendor form is required for all new vendors therefore effective controls are in place to manage this.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer.	**Implementation Date:** 29 March 2019

1.7 IR35 Training and awareness raising

Induction and refresher training for engaging managers should be designed and implemented to ensure that current and future engaging managers are fully aware of their IR35 responsibilities. This should include (but not be limited to) the requirement to consider and / or ensure:

- the employment status of temporary workers;
- services provided through partnerships;
- that assessments are performed and outcomes communicated prior to the start of the engagement; and
- that responses to queries received from workers and agencies regarding assessment outcomes should be provided within 31 days; and
- that all assessments are performed by the engaging manager and not the temporary employees.

Agreed Management Action

The current take-up of training across the Council is limited, therefore it is management's view that training would not be fully effective in addressing this risk. It is proposed that, in line with 1.8, the IR35 process and guidance available via the Orb will be revised to include all necessary requirements. Once revised, the revised guidance will be communicated across all the Council, with targeted communications for Service Areas who regularly use temporary workers.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant.	**Implementation Date:** 30 September 2019

1.8 IR35 Engaging Managers Guidance

In addition, IR35 'Off-payroll' content on the Orb should be revised to ensure it includes all points at recommendation 1.7, and instructions on the following:

- The requirement for the engaging manager to provide a copy of both the IR35 assessment and decision letter to either Commercial and Procurement Services (CPS) or Payroll when requesting payment to ensure evidence of assessments can be provided to HMRC if required;
- Additionally, to support this, the 'Off-payroll worker claim form' should be revised to include the requirement to attach the IR35 assessment and decision letter when requesting payment;
- The requirement for the engaging manager to manage the worker during engagement, including restrictions on the duties to be undertaken; and the requirement to reperform reassessments if the role or contract changes;
- Details of worker groups which are either IR35 exempt (for example, Foster Carers), or where a formal opinion on employment status has been obtained from HMRC (for example, Kinship Carers, Translators, and Curators Ad Litem). This should include the HMRC opinion for Daybreak Carers.

Agreed Management Action

As per 1.7, the IR35 process and guidance available via the Orb will be revised to include all necessary requirements. Once revised, the revised guidance will be communicated across all the Council, with targeted communications for Service Areas who regularly use temporary workers.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant.	**Implementation Date:** 30 September 2019

1.9 Monitoring and review of IR35 compliance

A risk based monitoring and review process should be designed and implemented to confirm the extent of ongoing compliance with IR35 requirements across the Council. Any breaches identified by either Commercial and Procurement Services (CPS) or Payroll should be reported to the relevant Heads of Service; Executive Directors; and the Corporate Leadership Team to ensure that appropriate remedial action is taken, and reported to HMRC where required.

Agreed Management Action

Commercial and Procurement Services (CPS) will, in collaboration with Payroll, monitor non-compliance with IR35 processes across the Council, and report on an exception basis to relevant Heads of Service to ensure remedial action is taken. Persistent breaches will be escalated to Executive Directors and the Corporate Leadership Team, and where required, reported to HMRC.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer; Grant Craig, Employee Life Cycle Lead Consultant; Linda Rowe, Payroll Specialist.	**Implementation Date:** 30 September 2019

2. Inclusion of IR35 responsibilities in contracts for agency worker suppliers — Medium

Review of the contractual arrangements for the agencies who supply temporary workers to the Council established that:

1. Pertemps

Management advised, that by arrangement, Pertemps only supply workers who are either paid directly through Pertemps payroll or employed via an umbrella company. Therefore, no IR35 assessment is performed as it does not apply to the engagement. We note however, this arrangement, has not been agreed formally in writing, either within the original framework tender documents, or within the final contract issued.

In addition, Pertemps does not provide confirmation of the payment status for individual workers (whether paid via their payroll or an umbrella company) prior to the start of an engagement on a routine basis. Consequently, as the responsibility to decide if off-payroll rules apply lies with the Council, there is no assurance IR35 responsibility has been discharged.

Pertemps has confirmed that it will be possible to provide this information going forward.

2. Other Agencies

Other agencies are used when Pertemps cannot meet recruitment requirements for a specific role. We reviewed a sample of three out of eight agency contracts established that (as with Pertemps) whilst informal arrangements were in place, contractual arrangements did not specify the processes to be applied by the agency to ensure effective discharge of the Council’s IR35 responsibilities.

Our review also noted the Council’s Terms and Conditions for Services issued when a waiver is granted does not include any reference to compliance with IR35 or intermediaries’ legislation.

Risks

- The Council cannot confirm that it has effectively discharged its IR35 responsibilities for workers engaged through recruitment agencies; and
- The Council could potentially be liable for penalties and payment of unpaid contributions to HMRC.

2.1 Formal Assurance from Pertemps

The Council should obtain formal written assurance from Pertemps that all current and future workers supplied to the Council will either be paid through Pertemps payroll or an umbrella company.

Agreed Management Action

A contract variation in relation to IR35 / intermediaries’ legislation will be drafted and issued to Pertemps to ensure the Council receives assurance over the employment status of current and future workers supplied.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Katy Miller, Head of Human Resources; Steven Wright, Lead HR Consultant; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Craig Russell, Principal Solicitor – Employment	**Implementation Date:** 30 September 2019

2.2 Assurance for other recruitment agencies

The Council’s Terms and Conditions for Services should be revised to include reference to IR35 / intermediaries’ legislation. This should include the requirement for the provider to confirm how the worker will be paid (i.e. self-employed, agency payroll or umbrella company). In addition, the Terms and Conditions should advise that where the worker is not paid via the agency payroll or an umbrella company, the Council will need to complete an IR35 assessment prior to employment commencing. The revised Terms and Conditions should be issued with all waivers.

The Council should also seek confirmation on the payment status of all workers currently supplied by other recruitment agencies.

Agreed Management Action

The Council’s Terms and Conditions for Services will be revised to include roles and responsibilities of both the Council and the recruitment agency in relation to IR35 / intermediaries’ legislation. The revised Terms and Conditions will be issued for all future waivers.

The Commercial and Procurement Services (CPS) Waiver Team will produce a list of all workers currently provided by other recruitment agencies and request that the engaging manager seeks confirmation from the agency on how the worker is paid.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Mark Crolla, Commercial Operations Officer; Craig Russell, Principal Solicitor – Employment	**Implementation Date:** 30 September 2019

3. Right to Work Compliance and Breach Reporting — Low

Right to Work Compliance

Review of a sample of 25 new employees and 10 employees with time limited right to work permission confirmed a high level of compliance with Home Office requirements. However, the following minor compliance issues were noted:

- For 1 worker, no documentation was held on file to demonstrate that the right to work check had been performed. Evidence was subsequently provided and added to the employee file;
- For 1 worker, while the date of the check was recorded within iTrent, it was not recorded on the validated copies of documents held within the employees file, in line with the Council's procedure; and
- Validated documents for 5 employees did not include the appropriate validation statement and signature of the manager completing the check in line with the Council's procedure.

Management have advised as the Home Office requirement is only to record the date of the check, they are considering removing the requirement to record the validation statement, date and signature on the copies of documents retained as this is now recorded electronically within iTrent.

Right to Work Breach Reporting

HR proactively monitors completion of right to work checks; issuing reminders to Service Areas to ensure follow-up checks are completed prior to expiry of time limited permission, and escalating instances of non-compliance to senior management for resolution. We note however, no Council wide reporting of overall compliance with right to work requirements has been produced since completion of the Employee Compliance project.

Management has advised that implementation of a suite of appropriate reports is currently being considered.

Risks

- The Council is unable to demonstrate full compliance with Home Office Right to Work legislative requirements;
- The Council cannot establish a 'statutory excuse' for employing an illegal worker; and
- The Council is liable to civil penalties, wider sanctions and reputational damage.

3.1 Recording the date of check in line with Home Office requirements

The Council is required to make a contemporaneous record of the date when the right to work check was conducted. Should the decision be made to remove the requirement for all recruiting managers to sign, date and record the validation statement, the Council will need to ensure the date recorded on iTrent is the *actual date* the check was conducted. Guidance on the Orb and within the Recruitment – manager guide should be updated and communicated to reflect this requirement.

Agreed Management Action

The Council will retain the requirement for recruiting mangers to sign, date and record the validation statement on the actual date the check was conducted. The Orb will be updated and communication sent to remind managers of this requirement.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant; James Bertram, HR Consultant.	**Implementation Date:** 30 September 2019

3.2 Monitoring and review of right to work compliance

Regular reporting should be developed to confirm the extent of ongoing compliance with right to work requirements across the Council. Any breaches identified should be reported to the relevant Heads of Service, and Executive Directors to ensure that appropriate remedial action is taken.

Agreed Management Action

We will implement regular reporting on right to work compliance, reporting six monthly on overall compliance across the Council and on an exception basis to relevant Heads of Service to ensure remedial action is taken to address any non-compliance. Persistent breaches will be escalated to Executive Directors.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant; James Bertram, HR Consultant.	**Implementation Date:** 30 September 2019

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on 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 the organisation's 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 4

The City of Edinburgh Council

Internal Audit

Public Sector Cyber Action Plan for Cyber Resilience Review

Final Report

9 April 2019

Overall report rating:

Significant enhancements required	Significant areas of weakness and non-compliance in the control environment and governance and risk management framework that puts the achievement of organisational objectives at risk

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk, and Best Value Committee in March 2018. 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 there to.

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

Digital technologies bring enormous opportunities for Scottish Public Services, but with them new threats and vulnerabilities that the Public Sector must effectively manage. The WannaCry ransomware attack in May 2017 that impacted areas of the NHS in Scotland and England, highlighted the seriousness of cyber threat to public sector organisations. The National Cyber Security Centre (NCSC) has also reported that the severity of cyber incidents affecting public (and private) sector organisations is likely to increase.

The Scottish Government has noted the importance of cyber resilience in Scotland's public bodies and has set forth a cyber resilience strategy which includes an action plan (the Public Sector Action Plan for Cyber Resilience (the Plan) to promote a consistent risk-based approach to cyber resilience across Scottish public bodies.

The Plan is a set of actions designed to strengthen cyber resilience, and has not been formalised as either legislative or regulatory requirements. However, implementation of the actions included in the Plan is strongly recommended by the Deputy First Minister.

The Scottish Government has requested that public sector organisations and their key partners confirm that assurance has been provided on their critical technical cyber controls by the end of October 2018, and can demonstrate progress toward implementation of the Plan actions by December 2018. Confirmation that these actions have been implemented will provide the Scottish Government with assurance that cyber resilience risks are managed consistently and effectively across the public sector.

The Council's Cyber Security framework and key cyber controls are managed and operated on behalf of the Council by their technology partner CGI.

Public bodies were encouraged by the Government to conduct a Cyber Essentials pre-assessment by end of March 2018. Completion of the pre-assessment enables organisations to identify whether their existing cyber security controls require remediation before applying for the cyber essentials certifications included in the Plan. There are two types of certification included in the Plan:

- Cyber Essentials - a self-assessment questionnaire covering 5 key controls: firewalls; secure configuration; access controls; malware protection; and patch management, and an external vulnerability scan to independently assess the adequacy of security, which is reviewed by an external certifying body; and
- Cyber Essentials Plus - this includes the same cyber security controls as Cyber Essentials, with additional verification performed by the external body to confirm the effectiveness of the controls through testing.

The Cyber Essentials Plus certification is the Scottish Government's preferred option where organisations cannot provide other alternative evidence of existing independent assurance on the effectiveness of their cyber security controls. Where independent assurance has been obtained on the effectiveness of the five critical cyber controls, Cyber Essentials is an acceptable alternative option.

Whilst the Plan focuses on cyber resilience, implementation of the actions will also support ongoing compliance with the requirements of the European Union's Directive on Security of Network and Information Systems (the Directive).

The Directive became effective in August 2016 and aims to increase cybersecurity resilience across Europe. EU member states had until 9th May 2018 to transpose the Directive into their national laws.

The Directive provides legal measures to enhance cybersecurity, particularly for industries and organisations that provide services essential to everyday life and the security of a nation. Specifically, the Directive aims to safeguard the supply of essential services that rely heavily on IT, such as energy, transportation, water, banking, financial market infrastructures, healthcare, and digital infrastructure.

Organisations in those sectors that are identified as operators of essential services (OESs) or digital service providers (DSPs) will be required to take appropriate security measures and comply with the incident notification requirements as set out by the Directive. These organisations will be required to report incidents to a regulatory authority and will face fines of up to £17m if breaches are due to failures in cybersecurity defences.

The NIS Directive will apply to all OESs and DSPs from 9th May 2018, with member states required to identify all OESs and DSPs in their country that are essential to the supply of electricity, water, digital infrastructure, healthcare, and transport by 9 November 2018. It has not yet been confirmed whether the requirements of the Directive will be extended to Scottish local authorities.

In addition to the Directive, implementation of Plan actions will also support ongoing compliance with new General Data Protection Regulations (GDPR) that became effective in May 2018,

Consequently, public sector organisations should also consider how their cyber resilience and technical cyber controls align with both Directive and GDPR requirements on an ongoing basis. Whilst the Council's Customer and Digital Services team will be responsible for confirming to the Scottish Government that Plan actions have been implemented, effective cyber Security resilience is priority for all Service Areas across the Council, as the Plan also includes governance; risk; and supply chain recommendations.

Failure to achieve at least Cyber Essentials accreditation by October 2018, and demonstrate progress with implementation of the actions included in the Plan by December 2018 could result in potential adverse reputational damage for the Council.

The Scottish Government has published the following 11 key actions for public sector organisations (https://www.gov.scot/Publications/2017/11/6231/2) to work towards alignment with their cyber resilience strategy. 8 of the 11 key actions had been issued by the government at the time of our review:

1. To adhere to the Public Sector Cyber Resilience Framework requirements (note that these requirements had not been at the time of our review);
2. To have minimum cyber security Governance arrangements in place by June 2018;
3. To promote awareness of cyber threats and intelligence;
4. To have appropriate independent assurance of critical technical controls and defences;
5. To make use of National Cyber Security Centre (NCSC) Active Cyber Defence Programme by June 2018;
6. To set up appropriate staff training and awareness and disciplinary procedures. Government Document and guidance to be provided by June 2018;
7. To adopt cyber incident response process and protocols;
8. To adopt a proportionate risk based security view of the supply chain (note that the SG supply chain cyber security policy has not yet been issued);

9. To ensure appropriate access to expertise in supporting public bodies on cyber resilience, the Scottish Government will put in place an Innovative Dynamic Purchasing System for Digital Services;
10. Participate in the creation of the Public Sector Cyber Catalyst Scheme; and
11. To apply the monitoring and evaluation framework designed by the SG to monitor progress against this action plan. This had not been issued at the time of our review.

Scope

The objective of this review was to assess the Council's progress towards Cyber Essentials accreditation by end of October 2018, and progress with delivery of the Plan actions (detailed above) by December 2018.

We also reviewed the independent assurance provided as part of the Cyber Essentials pre-assessment process to confirm whether appropriate actions are planned to address any significant control gaps identified.

Our work was performed during August 2018 and concluded by the end of August. Our opinion and the findings included in this report are based on the outcomes of our work as at **31 August 2018**.

Limitations of Scope

- This review focused only on the design of the Council's cyber security controls that are relevant for the Plan. No detailed testing was performed to determine their effectiveness;
- Only those processes and policies within the control of the Council and CGI were included in scope. Cyber security controls applied by third party organisations supporting Council services are excluded as the Plan is not yet clear on these requirements;
- Cyber security controls in relation to the Public Services Network (PSN) provided by the UK government were specifically excluded from the scope of this review. PSN compliance will be assessed within the scope of our planned review of 'Out of Support Technology and Public Services Network Accreditation'; and
- Our work does not guarantee that the organisation will be fully compliant with requirements of the Plan.

2. Executive summary

Summary of findings raised	
High	1. Critical Operational Cyber Security Controls
Medium	2. Key Cyber Security Controls Monitoring
Medium	3. Public Sector Cyber Action Plan Project Governance

Opinion

The City of Edinburgh Council ("the Council) recognises Cyber Security as high priority and acknowledges that the Scottish Government (SG) wants Scottish public sector bodies to become exemplars in cyber resilience. The Council confirmed in their covering letter to the Scottish Government in July 2018 (supporting submission of their baseline cyber security questionnaire) that they will initially aim for Cyber Essentials (CE) accreditation, with CE plus accreditation post October 2018.

Areas for Improvement

Our review has confirmed that significant enhancements are required to ensure that the Council achieves Cyber Essentials (CE) accreditation by end of October 2018, and can demonstrate progress with delivery of expected Plan actions by December 2018.

This opinion reflects a number of known significant weaknesses in existing key cyber security operational controls; the need to establish and ensure ongoing monitoring of the effectiveness of the Council's full population of cyber security controls; and the need to confirm whether areas of the Council that operate standalone networks (for example, schools and the Lothian Pension Fund) and other standalone systems (such as the EDINDEX system used by citizens to submit applications for Council property) will be included in the scope of the Council's applications for accreditation.

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

Progress to Date

Whilst a number of significant control enhancements are required to achieve and support the implementation of the cyber actions detailed in the Plan, it is important to note that the Council has already met a number of expected Plan timeframes. These include:

- Completion of the independent Cyber Essentials Pre-Assessment test and receipt of the results by April (a prerequisite of action 4);
- Submission of the initial SG Public Sector Action Plan for Cyber Resilience baseline questionnaire in July 2018, confirming current progress against the Plan, and providing details of ongoing cyber remediation work;
- Establishing minimum cyber security governance arrangements by June 2018 (action 2), through formation of the Cyber Information Security Steering Group (CISSG);
- Progress on staff training and awareness through ongoing campaigns and phishing training (action 6); and
- Participation in the Public Sector Cyber Catalyst Scheme (action 9).

Areas of Good Practice

Whilst we identified a number of areas for improvement, the following areas of good practice were also noted during the review:

- Establishment of strong ongoing dialogue with both the SG and the SG Cyber Resilience Unit;
- Attendance at SG training and Public Sector Cyber Catalyst meetings designed to facilitate knowledge sharing and identification of practical cyber security solutions;
- Regular consideration of both cyber and information security risks by the Council's Corporate Leadership Team;
- Formation of the Cyber Information Security Steering Group (CISSG) in June 2018 with representation from all Council Directorates; Information Governance; and CGI;
- A proactive approach to GDPR has been adopted; and
- SG recognition that the Council's cyber security training is exemplary. and there is opportunity to replicate it across other public sector organisations.

3. Detailed findings

1. Critical Operational Cyber Security Controls	High

Our review confirmed that remediation work in relation to key cyber security controls is ongoing, with completion timeframes that currently extend past the planned Council's Cyber Essentials and Plan completion dates. We have outlined the following findings that relate to actions 4 and 5 from the Public Sector Action Plan for Cyber Resilience (see Background section for details of the of actions) as they relate to independent assurance over critical controls and the NCSC defence programme. Specifically:

- **Patch Management (action 4)** – Whilst the Council has implemented a monthly patch management regime for WINTEL and UNIX servers, the results of the Pre-Assessment conducted in March 2018 for Cyber Essentials confirmed that the Council would not qualify for Cyber Essentials Plus accreditation without appropriate, timely, and fully effective patch management remediation;

- **Legacy Operating Systems and Unsecure Software (action 4)** – The Council currently uses legacy operating systems and unsecure software that increases exposure to cyber attacks, and impacts patch management as patches are generally only available for current and most recent versions.

  A technology refresh programme has commenced and is expected to complete in June 2019. This programme will replace all of the Council's end user devices across the estate, ensuring that only fully supported software applications are used and supported with effective ongoing patch management controls. If the programme cannot be delivered in line with expected Plan timeframes, reliance could be placed on compensating vulnerability scanning controls, however, our review has confirmed that these controls are currently not effective.

- **Vulnerability Scanning (action 4)** - Manual vulnerability scanning is currently being performed by CGI, with the most complex aspects of the work to be completed in September 2018. CGI has advised that real-time vulnerability scanning tools will be in place by November 2018, however this implementation date has been consistently revised.

  Lack of ongoing vulnerability scanning was also noted as an outstanding item raised by Scott Moncrieff as part of their 2016/17 external audit technology controls work;

- **Shadow IT (action 4) –** Customer and Digital Services compiled a list of all shadow IT (bespoke systems or applications that are not supported by CGI) used across the Council based on information provided by Service Areas in October 2017. To prohibit future purchase of shadow IT, reliance is placed on existing procurement controls, however, procurement controls do not prevent the purchase of shadow IT where the cost is less than the £3K procurement threshold required for approval.

  Whilst technology controls exist to prohibit Council staff downloading software on to devices, and Web Check is used to scan for website vulnerabilities, cyber security risks associated with shadow IT cannot be effectively managed and will not be fully mitigated until completion of the technology refresh programme that will address the risks associated with legacy software, and implementation of ongoing real-time vulnerability scanning;

- **Network Segregation (action 4)** - The Council has confirmed that the schools network will be excluded from the Public Sector Action Plan for Cyber Resilience on the basis that this is a stand-alone network. The CGI contract includes specific Output Based Specifications (OBSs) relating to network management, and includes responsibilities for monitoring the segregation of network traffic, which is achieved through Virtual Routing and Forwarding (a network router that enables network paths to be segmented without using multiple devices). Whilst CGI has provided written confirmation to confirm segregation between schools and the core council network, no evidence has been provided to support this view.

- **Domain Name System Controls (action 5)** – A Public DNS is one of the National Cyber Security Centre (NCSC) Active Cyber Defence Programme recommended tools. When connecting to networks or websites, a DNS directs users to the correct server location/IP address by accurately translating domain names.

  The Council's existing Domain Name System (DNS) is situated internally within the Council's network and is not designed to support an externally hosted DNS as recommended by NCSC (Plan action 5). The existing DNS requires manual intervention when there is a switch over to a secondary infrastructure.

  CGI has confirmed that the DNS cannot be enhanced without significant network redesign as the Council's network is not designed to access an externally hosted DNS such as the Public DNS recommended by NCSC. Whilst compensating controls have been established, these will only prevent redirection to known malicious sites

  No analysis has been performed to assess whether the current internal design is any less secure than the recommended Public DNS tool.

- **User Access Controls (action 4)** - Whilst significant progress is evident with improving user access controls (such as removal of desktops from the network after 30 days of inactivity), outstanding actions identified by Scott Moncrieff as part of their 2016/17 external audit technology controls review are only partially complete. These relate to privileged user accounts for Wintel and UNIX operating systems; and the requirement to update the UNIX password policy to align with the Council's policy.

Risks

- The Council may be unable to provide assurance over critical cyber security controls and may not achieve Cyber Essentials accreditation and by October 2018;
- The Council may be unable to demonstrate adequate progress towards implementation of the Public Sector Action Plan for Cyber Resilience actions by 31 December 2018; and

  If the DNS is not operating effectively or is comprised, this can result in changes to the IP address with users redirected to unknown malicious sites. Another risk is that anti-virus software can also be jeopardised, which means networks may not be adequately protected against malware.

1. Recommendation - Cyber Essentials Accreditation

1.1. A decision should be taken as to whether it is realistic to aim for CE plus accreditation in 2019, as the Technology Refresh Programme that will resolve known patch management issues is not scheduled to complete until June 2019; and

1.2. CE Plus accreditation may still be possible if reliance is placed on the effectiveness of compensating vulnerability scanning controls across the Council's networks, however, assurance should be obtained from CGI that the current manual vulnerability scanning will be completed on schedule by the end of September 2018, with automated scanning implemented and fully operational by November 2018, supported by an appropriate remediation process to ensure that all vulnerabilities identified are addressed in a timely manner.

Agreed Management Actions - Cyber Essentials Accreditation

1.1. CE Accreditation was achieved October 2018. Based on the advice received, we are therefore continuing with the current plan for Cyber Essentials Plus accreditation in 2019. We are dependent on some improvement plans and programmes by CGI that are tracked via the Public Services Network Board and Security Working Group.

1.2. CGI 's progress will be reviewed at the end of January 2019 and monthly afterwards.

1.3. A formal review to assess whether accreditation can be achieved will be completed by end March 2019 by the Enterprise Architect with support and oversight by the Chief Information Officer. A proposal to continue for submission will be then made by the CIO, to the Head of Customer and Digital Services, and the Executive Director of Resources.

1.4. CGI completed a complete manual vulnerability scan of the estate in November 2018 Vulnerabilities identified from this scan are being resolved as part of the Public Services Network remediation action plan. CGI have been formally requested to implement automated vulnerability scanning as a service. To ensure this is in place in time for Cyber Essentials Plus accreditation this automated vulnerability scanning is targeted to be implemented by end of June 2019.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 30 September 2019

2. Recommendation – network segregation

2.1 Evidence should be requested from CGI to support their confirmation that the schools network remains effectively segregated from the main Council network. This should include details of the testing performed, and a summary of the outcomes; and

2.2 Ongoing confirmation of network segregation (based on testing) should also be either requested every six months, or in the event of any significant changes to the design of the network architecture.

Agreed Management Action – network segregation

2.1 CGI have confirmed in writing that our networks are segregated. We will also provide additional evidence of network segregation between the Corporate and Learning and Teaching networks. We will raise a change request to ask CGI to carry out PING tests from a selection of 20 representative schools to see if they can locate corporate network assets.

The PING test will confirm whether the content of one server can be viewed from another. If nothing can be viewed, this means that the servers cannot be accessed as they are appropriately segregated.

We will raise the appropriate request 28th February 2019 and ask CGI to complete the work by the end of June 2019.

If the PING tests prove that the networks are appropriately segregated, then no further action is required in relation to Cyber Essentials Plus accreditation. If the networks are not appropriately segregated, then a proposal will be made to the Corporate Leadership Team to either combine the networks, or include the schools and learning network within the scope of Cyber Essentials Plus accreditation.

2.2 A process will be agreed with the CGI Network team to repeat the PING tests in the event of significant change to network architecture. This will be managed through the Network Improvement Working Group, and will be included in the change request noted above.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 30 September 2019

3. Recommendation - Domain Name System Controls

3.1 A gap analysis should be performed in conjunction with CGI to assess the gaps between the current internal DNS and the Public DNS solution;

3.2 The outcomes of the gap analysis should be used to determine whether the Public DNS solution should be fully or partially implemented;

3.3 The decision in relation to the DNS solution should be based on an assessment of the risks associated with each option, and a supporting cost and benefit analysis;

3.4 If the DNS approach is to be changed, a supporting implementation plan should be developed and applied; and

3.5 DNS controls should be tested to ensure that they are operating effectively prior to implementation.

Agreed Management Action – Domain name system controls

3.1 **Action 1** - We have requested that CGI provide a gap analysis by 28th February 2019. The output will be provided to audit.

3.1.1 On the basis of this, recommendations to consider PDNS implementation in part or completely, or whether we will continue the with current DNS solution will be provided to the Head of Customer and Digital Service; the Executive Director of Resources. With a recommendation by 14th March 2019. Evidence of the gap analysis, recommendation and decision will be provided to audit.

3.1.2 Risks will be considered as an integral part of the decision making process, with cost impacts to change included in determination. If the decision is take not to not implement the PDNS, the risk will be captured on the ICT risk register, and managed through the risk management framework.

3.2 **Action 2** - If the decision is taken to implement PDNS then the following agreed management actions will be raised and an implementation date agreed.

3.2.1 A supporting implementation plan will be developed and considered as part of the decision making process

3.2.2 A Change request (CR) will be raised as necessary with CGI to formulate an Implementation Plan in the event of a decision to change to PDNS. The CR will be raised following the conclusion of Action 1 directly above.

3.2.3 The tool will be fully tested prior to implementation to confirm that it is operating as expected prior to go live.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date for Action 1: 31 May 2019

Agreed Implementation Date for Action 2: to be determined when the decision is taken in relation to PDNS implementation.

4. Recommendation – User access controls

4.1 Formal confirmation and supporting evidence should be requested from CGI that external audit recommendations in relation to privileged user accounts for Wintel and UNIX operating systems; and the requirement to update the UNIX password policy to align with the Council's policy have been addressed prior to completing CE Plus accreditation.

Agreed Management Action – User Access Controls

4.1 CGI indicated that the full recommendations made by the external auditor could not be implemented without significant change to the contract and at a notable additional cost.

CGI provided the Council and the External Auditors with details of the current oversight of the CGI Wintel and UNIX password policies.

Current ongoing evidence of this oversight via the SWG will be provided to external audit, a statement confirming the risk acceptance by the Executive Director of Resources will be prepared, approved, signed, and provided to Scott Moncrieff.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 31 May 2019

2. Cyber Security Controls Monitoring

Medium

The Scottish Government expects public sector organisations to ensure they have in place appropriate independent assurance over critical cyber security controls by the end of October 2018. The Council is dependent on their technology partner CGI for identification and confirmation of the ongoing operating effectiveness of these controls.

To date, the full population of the Council's critical cyber security controls has not been fully identified, and reporting on their ongoing effectiveness established. Monthly security reports detailing the operational performance of some key controls (for example, patch management which is a high risk area for the Council due to the volume of legacy IT estate) are received from CGI and reviewed by ICT.

Whilst management acknowledges that the content and quality of the security reports is improving, review of a sample of reports confirmed that their format is inconsistent; they include inaccurate data; and performance dashboards are not consistently populated.

Additionally, performance of recently implemented cyber controls is not being monitored due to delays in implementation and reporting. For example, a new Intrusion Prevention System (PIPS) was implemented between February and June 2018, however CGI have yet to provide any reporting on the effectiveness of its operation.

Risk

- The Council will be unable to monitor the ongoing effectiveness of cyber security controls; resulting in the inability to monitor trends; identify and prioritise remediation of control gaps; and report to findings to senior management;
- The Council may be unable to provide assurance over critical cyber security controls and may not achieve Cyber Essentials accreditation and by October 2018; and
- The Council may be unable to demonstrate adequate progress towards implementation of Plan actions by 31 December 2018.

1 Recommendations - Cyber Security Controls Performance Dashboard

1.1 Establish and implement a cyber security control performance dashboard (based on agreed key performance indicators) that includes the full population of preventative; detective; and compensating controls operating across the Council covering the SG five key critical Plan cyber security themes (firewall; secure configuration; patch management; access management; and malware) in conjunction with CGI, that measures the effectiveness of their ongoing operational performance.

Agreed Management Action - Cyber Security Controls Performance Dashboard

1.1 The council agreed a dashboard for reporting on key controls as part of previous internal and external audits. This forms part of the monthly SWG Service report. The Council has requested that a record of firewall rules reviews and intrusion prevention and detection controls (detailing all attempts made to gain access through internal and external firewalls) are included in the dashboard.

As at December 2018, CGI has not been able to provide a consistent and complete report for a continuous period of 3 months. This was escalated within the established partnership escalation procedure, and now appears to have been resolved, however, Digital Services are monitoring for a period of 3 months from Jan to March 2019 to confirm that the reports are complete and accurate.

There is one exception to this as CGI currently do not provide vulnerability scanning as a Service. This is covered in Finding 1.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 31 July 2019

2. Recommendations - Escalation and Resolution of Operational Performance Issues

2.1 Ensure that any significant weaknesses in the operational performance of these controls are escalated by the Security Working Group to the Partnership Board for resolution within specified timeframes; and

2.2 Weaknesses in the operation of key cyber security controls will be reflected in the CISSG risk register (refer finding 3 below)

Agreed Management Action - Escalation and Resolution of Operational Performance Issues

2.1 We believe escalations around operation matters are via the SWG and then the CEC/CGI escalation procedure to either the Partnership Board or the Executive Review Board. We have evidence this has happened.

2.2 Issues around vulnerability will continue to be recorded in the ICT Risk log (as is done now) and where appropriate will be recorded in the CISSG Risk Log as is proposed.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: Now complete. 30 April 2019 (for IA validation).

3. Public Sector Action Plan for Cyber Resilience Project Governance	Medium

Whilst a Public Sector Action Plan for Cyber Resilience tracker and risk log has been established detailing the requirements to achieve CE; CE Plus; and implementation of Plan actions, detailed timeframes and the risks and dependencies associated with timely delivery have not yet been recorded and presented to the CISSG and the Corporate Leadership Team (CLT). These include:

- Lack of clarity regarding the scope of the Council's accreditation; subsequent CE plus accreditation and implementation of Plan actions will include areas of the Council that operate stand alone networks (for example, schools and the Lothian Pension Fund) and other stand alone systems (such as the EDINDEX system used by citizens to submit applications for Council property).
- Dependency on the Council's technology partner CGI for delivery of 2 strategic IT programme initiatives: the upgrade to Office 365 across the technology estate (scheduled to complete November 2018); the refresh of all technology devices and hardware (initially scheduled to complete June 2019, although will be likely extended given the volume of devices and hardware included in the Council's legacy technology estate); and remediation of known weaknesses in existing cyber security controls.

  Progress updates provided by CGI are not yet clear on completion timeframes for the technology refresh programme and remediation of known weaknesses in key cyber security controls;
- Lack of a consolidated thematic technology risk register that provides a holistic view of cyber security risks and the effectiveness of supporting controls across the Council, and no assurance (as yet) that Service Areas are effectively managing their own cyber security risks;

  Whilst plans have been developed to support delivery of a thematic risk register (for example, workshops facilitated by Risk Management for Heads of Service), no timeline for completion has been established;
- Timeframes for completion of the independent accreditation (Public Sector Action Plan for Cyber Resilience action 4) have been consistently revised, and no supplier has yet been engaged to perform the assessment.

  Management has confirmed that CGI has identified a preferred supplier, although arrangements for the independent accreditation review have not yet been confirmed given known and ongoing challenges with the technology refresh programme and remediation of known weaknesses in existing cyber security controls;
- Known difficulties in monitoring training completion rates due to incomplete and inaccurate employee data, which is restricting the analysis of training attendance; progress reporting to the CISSG; and provision of feedback to Service Areas. Additionally, as the Council does not apply a mandatory training approach, reliance is placed on managers and employees to take a proactive approach to complete the training.

  This issue has already been raised as a Medium rated finding in the Phishing Resilience Internal Audit review completed July 2018, and management is working to an agreed implementation date of 29 March 2019, which provides a significant challenge in relation to successful and timely delivery of Public Sector Action Plan for Cyber Resilience action 6.

Risks

- Until a thematic technology risk register is established, existing Council wide cyber security risks cannot be addressed;

- The Council may be unable to provide assurance over critical cyber security controls and may not achieve Cyber Essentials accreditation and by October 2018; and
- The Council may be unable to demonstrate adequate progress towards implementation of Plan actions by 31 December 2018.

1 Recommendations - Public Sector Action Plan for Cyber Resilience Project Scope

1.1 The scope of the Council's Public Sector Action Plan for Cyber Resilience project should be clearly defined, and agreement reached on whether this should include areas of the Council that operate standalone networks and systems.

Agreed Management Action - Recommendations - Public Sector Action Plan for Cyber Resilience Project Scope

1.1 The Council does not have 'standalone' networks. The Plan scope in general covers all services that are provided via the Council's Corporate and Learning and Teaching Networks. Cyber Essentials has been obtained on that basis. It is proposed that Cyber Essentials Plus will only be submitted for systems within the Corporate Network.

The Plan Council's Plan accreditation work does not include any systems that are hosted externally to the above networks.

This is being communicated to the Deputy First Minister in a response to be sent by the Council in December. Action complete and evidence to be provided

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: Completed - 30 April 2019 (for IA validation)

2 Recommendations - Public Sector Action Plan for Cyber Resilience Project Plan

2.1 The existing Plan project tracker and risk log should be enhanced to ensure that it reflects current timeframes for all CE Plus and Plan activities, including key dependencies on other projects / programmes and third party suppliers; and

2.2 CE plus and Plan action timeframe extensions should be discussed and approved by the CISSG, with the supporting rationale for the decision documented; approved by senior management and an explanation logged.

Agreed Management Action - Public Sector Action Plan for Cyber Resilience Project Plan

2.1 Complete - the existing Plan project tracker and risk has been enhanced to ensure that it reflects current timeframes for all CE Plus and Plan activities (including appointment of an independent accreditor once timeframes for CE Plus accreditation have been agreed), including key dependencies on other projects / programmes and third party suppliers.

2.2 As with Cyber Essentials, the Cyber Essentials Plus submission will be approved through the appropriate channels i.e. through the CIO; the Head of Service; the Director; the Security Working Group (SWG) and wit the CISSG kept informed. This will be further reviewed formally at end of March 2019

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 30 April 2019

3 Recommendations - Thematic Cyber Security Risk Register

3.1 Timeframes for completion of planned risk workshops and design and implementation of a thematic technology / cyber security risk register should be finalised;

3.2 The risk register should reflect all known and significant potential Council wide cyber security risks; details of established cyber controls and an assessment of their effectiveness as advised by the relevant service risk owners; with ownership, actions, and timeframes to address the risks allocated and documented; and

3.3 Once created, the risk register should be regularly updated and the effectiveness of key controls regularly assessed by the relevant service risk owners on an ongoing basis (at least quarterly).

Agreed Management Action - Thematic Cyber Security Risk Register

The Internal Audit recommendations at 3.1 to 3.3 above will be implemented

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nick Smith, Head of Legal and Risk; Duncan Harwood, Chief Risk Officer; and Rebecca Tatar, Principal Risk Manager

Agreed Implementation Date: 30 September 2019

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: - ***Critical*** impact on 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 or brand 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 or brand 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 or brand of the organisation.
Low	A finding that could have a: - ***Minor*** impact on the organisation's 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.

Appendix 5

The City of Edinburgh Council
Internal Audit

Street Lights and Road Traffic Signals

Place

Final Report

31 January 2019

Project Code: PL1810

•EDINBVRGH•
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018 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 City of Edinburgh (the Council) provides and maintains a total of 64,000 street lights and 605 traffic signals across the City. It is the Council's duty to ensure that these are operated and maintained appropriately and in accordance with all relevant regulation and standards.

Street Lighting

Where the Council decides to provide street lighting, it must do so as per the requirements of s35 of the Roads Scotland Act. British Standards and Well-lit Highways codes of codes of practice also specify the requirements to electrically test electrical apparatus every 6 years.

Street lights have different lifespans, and current Council policy is to start structural testing columns within 6 years of end of design life and 6 every years thereafter on steel or concrete posts. New aluminium posts have a maintenance life of 40 years. There is currently a rolling programme of maintenance for all street lamps across the city. Once complete all necessary posts will have been electrically and structurally tested and where necessary repaired or replaced.

Elements of the ongoing street lighting operation and maintenance are performed by external suppliers. Mallatite is the street lighting aluminium column manufacturer; and Electrical Testing Ltd performs structural testing on street lighting columns.

In June 2018, the Council embarked on a three year project to upgrade street lighting to new energy efficient lanterns which have a life of circa 100,000 hours (25 years). Around 10,000 street lights already have energy efficient lanterns fitted and the project will replace the remaining 54,000. The upgrade is estimated to avoid CEC £54m of energy, maintenance, and disposal costs over 20 years, and will be delivered by an external supplier (Amey).

The street lighting inventory is maintained on the Confirm system. Management has advised that the Confirm inventory is not complete, and that it will be upgraded (as part of the street lighting upgrade), with implementation of electronic handheld devices that interface with the inventory system. The inventory update will be performed on a street by street basis to ensure that the full population of street lights are recorded.

A paper detailing the street lighting and management arrangements applied by the Council was presented to the Transport and Environment Committee on 9 August 2018 Street Light Management Arrangements Paper.

Traffic Management

There are currently 605 traffic signals in use across the City, designed to meet all applicable UK and local standards. All traffic signal equipment must have UK type approval in line with the TR suite of specifications or the recently introduced TOPAS (Traffic Open Products and Specifications) approval process.

An external supplier (Siemens) has been engaged to perform the annual electrical testing and ongoing traffic signal maintenance. Monthly meetings are held with Siemens to discuss testing progress and any other issues. Rebates are included within the contract and penalties applied where annual electrical testing requirements or issue resolution timeframes are not achieved.

The Siemens 'InView' hosted fault and asset management system is used to record, monitor, and maintain all traffic signals operated by the Council. InView is updated with all electrical testing results, and is also used to log and track the status of operational issues, and record information for individual traffic signals, for example, electrical testing certificates.

One third of the City's traffic signals are linked to the urban traffic control (UTC) centre which enables remote adjustment of non-safety critical timings, and supports the remote introduction of timing changes and plans aligned with demand (am peak, off peak, evening peak).

There is a contract in place with Dynniq (UTC system supplier) to provide ongoing maintenance and support, including an annual system 'health-check'. UTC access is restricted via password control and can be accessed remotely via Council terminals, and laptops. Standby engineers also have remote dial in access. A back-up process has also been established to ensure that UTC system data can be recovered in the event of a system failure.

All new traffic signals must be designed and programmed to reflect the bespoke nature of each junction/crossing. Once programmed, factory and site acceptance tests (including electrical testing) are performed to confirm that all safety and operational parameters are performing effectively. Any significant testing issues would result in rejection of the equipment.

Where new signals are linked to the UTC, the traffic signal controller is programmed with the required data (outlined within the TR2500 specification). The UTC in-station is also programmed to accommodate the new junction.

The UTC is also used to support the Tram signalling system. The Council and Tram signalling networks within UTC are completely segregated.

The UTC also highlights some traffic signal faults and retains a log of all faults identified to support resolution tracking. All faults are reported to the office, with out of hours faults reported via CLARENCE (customer lighting and roads enquiry centre). The Contact centre uses guidance provided by Transport to prioritise emergency repairs. A team of in house engineers (who have remote access to the UTC) is on 24 hour standby for any emergency repairs, and support is also provided by Siemens engineers under an agreed maintenance contract.

The remaining traffic signals are stand alone, with signal timings programmed into the local traffic signal controllers that are secured by a universal lock, preventing other utility providers from accessing the box.

Scope

The scope of this review assessed the design adequacy and operating effectiveness of controls established to maintain and manage the Council's street lighting and road traffic signals, with focus on supplier management; compliance with applicable regulations and standards; traffic and street lighting testing; inventory maintenance;); and resolution of requests for service.

Sample testing was performed during the period 27 August to 30 September 2018. Our review concluded on 12 October 2018, and our opinion and findings are based on the outcomes of our testing at that date.

2. Executive summary

Total number of findings: 5

Summary of findings raised	
Medium	1. Traffic Signals: UTC system access controls
Medium	2. Street Lighting: Inventory and maintenance
Low	3. Street Lighting and Traffic Signals: Process and quality assurance documentation and training
Low	4. Traffic Signals: Evidence of pre installation design and acceptance testing
Low	5. Traffic Signals: Supplier management framework

Opinion

Our review confirmed that the control environment established to support the ongoing maintenance and management of street lighting and traffic signals is generally adequate, with enhancements required, as some moderate and minor control weaknesses were identified.

Areas for Improvement

The moderate control weaknesses reflect the need to ensure that UTC (the system used to remotely manage the Council's traffic signals) access controls are improved and that all annual UTC health checks are performed by the system supplier; street lighting inventory records are accurately maintained to support completion of ongoing maintenance in line with applicable regulatory and statutory requirements; and the outcomes of ongoing street lighting structural testing is accurately recorded.

The minor control weaknesses highlighted that there is currently no established operational process documentation supporting ongoing maintenance of street lighting and traffic signals; the quality assurance pack requires to be updated; and that no role specific induction training is in place for new team members. There is also a need to ensure that the nature and outcomes of pre installation traffic light testing is recorded; and that monthly supplier management meetings with the external contractor responsible for ongoing traffic signals electrical testing are reinstated.

Consequently 2 Medium and 3 Low rated Internal Audit findings have been raised.

Areas of Good Practice

It is also important to note that a number of areas of good practice were identified during our review. These included:

- Timely submission of annual usage / consumption reports to the Association for Public Service Excellence (APSE) and Whole Government Accounts;
- Timely completion of traffic signal annual electrical testing had been performed on a timely basis with all relevant documentation completed.
- Historic street lighting faults reported prior to implementation of the Confirm system have been recorded and necessary repairs are being scheduled. This process is operating effectively and is also being used to monitor completion of repairs for emergency faults.

Our detailed findings and recommendations are laid out at **Section 3** below.

3. Detailed findings

1. Traffic Signals: UTC system access controls	Medium
The Urban Traffic Control (UTC) system (used to remotely manage the Council's traffic signals) is accessed by all team members and remotely by stand by engineers using the same user identification and password. UTC system functionality provides access for multiple users with unique user identifications and passwords, however, the Council does not use this functionality, and there is no system audit trail detailing UTC changes made by users. Additionally, no ongoing system access reviews are performed to ensure that only authorised employees continue to have access to the system. Finally, annual UTC system health checks were not performed by Dynniq in 2017 and 2018. The last annual health check was completed in early 2016 (the health check report was dated May 2016).	
Risk	
• Inappropriate UTC access could result in unauthorised changes that could adversely impact operation of the traffic signals network, resulting in reputational damage; • System input errors cannot be traced to system users; and • System issues and bugs may remain undetected and could potentially result in system failure.	
1. Recommendation – UTC User access controls and user profiles	
Urban Traffic Control (UTC) centre user access functionality for multiple users with unique user identification and password controls should be implemented; with all employees allocated user profiles that reflect their roles and responsibilities (for example, read only; review; and approval access).	
Agreed Management Action	
Use of unique user identification and password controls will be introduced, with appropriate access levels assigned to approved users, however, the requirement to change passwords regularly will not be introduced as reliance is placed on access to Council networks to access the Urban Traffic Control Centre (UTC).	
Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.	
Implementation Date: 30 April 2019	
2. Recommendation – UTC Unauthorised users	
Where unauthorised users are identified (for example employees who have left or changed roles) their access rights should be removed.	
Agreed Management Action	
Access rights will be removed for staff leaving (or changing) roles with access rights for all users reviewed annually. An annual frequency is appropriate as users require access to the Council network	

in order to access the UTC. If leavers are removed from the Council network, they would need to download the UTC application onto a personal device to maintain access to the system.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: By 30 September 2019.

3. Recommendation – UTC annual system health checks

Management should liaise with Dynniq to ensure that annual UTC system health checks are performed and review and discuss the outcomes with the supplier.

Agreed Management Action

Dynniq to be instructed to undertake an annual UTC system health check prior to the end of the current support contract. Evidence of annual health check to be recorded on InView, and a management review performed annually to ensure that all health check actions have been completed and recorded on InView.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: By 31 May 2019.

2. Street Lighting: Inventory and maintenance — **Medium**

The street lighting inventory system, Confirm, is not complete and accurate. Management has advised that they are aware of this issue and have established plans to update the inventory as part of the wider street lighting upgrade project which will be delivered by contractors (Amey), and is scheduled to commence in October 2018.

We established that Electrical Testing Ltd (who are contracted to complete the street lighting structural testing) use several databases to publish their testing results, which creates challenges in monitoring and reconciling completed testing with outstanding testing.

Review of a sample of 16 street lights that had been subject to testing highlighted the following exceptions:

1. Five street lights had not been added to the Confirm inventory;
2. Two were added to works orders in error;
3. Two were awaiting addition of test certificates on Confirm following works completed in June 2017 and June 2018 respectively;
4. One was included in the inspection programme but had not been inspected since 1998, failing the 6 year inspection criteria;

Finally, we established that Confirm system automated and remote update functionality is not being consistently used by Edinburgh Road Services Frontline Teams, with the system being updated manually.

Risk

- Ongoing street lighting monitoring and maintenance is not performed resulting in failure to comply with applicable legislation and potential breach of statutory Health and Safety obligations in the event of light failures;
- Increased volumes of emergency repair requirements if routine ongoing maintenance is not performed; and
- Inaccurate reporting of energy consumption figures to Scottish Power, resulting in potential financial and reputational consequences if penalties are imposed.

1. Recommendation – Street lighting inventory completeness and electrical testing results

Clear processes should be designed and implemented to ensure that all street lighting additions and removals are accurately recorded on the Confirm system, and that electrical testing outcomes are completely and accurately recorded on Confirm, with testing progress accurately monitored and reconciled. These procedures should be included in relevant operational procedure manuals (refer recommendation 3 below); and

Agreed Management Action(s)

Clear processes will be designed and implemented to ensure that:

- all street lighting additions and removals are accurately recorded on Confirm;
- electrical testing outcomes are completely and accurately recorded on Confirm; and
- progress with testing is accurately monitored and reconciled.

These processes will be included in the Street Lighting Operational Guide (developed under Finding No 3 below).

With this action being inextricably linked with the ongoing Energy Efficient Street Lighting Programme, implementation will be phased (on a Ward by Ward basis) within six months of completion of each Ward within the Programme, with full completion by 30 June 2022.

It has been agreed with Internal Audit that an implementation date of 20 December 2019 has been agreed with Internal Audit, enabling them to perform sample testing across the wards that have been completed at that time.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: 20 December 2019

2. Recommendation – Street Lighting Inventory Checks

Following completion of the street lighting, ongoing (monthly or quarterly) inventory checks should be implemented to confirm the completeness and accuracy of the inventory recorded in the Confirm system.

With this action being inextricably linked with the ongoing Energy Efficient Street Lighting Programme, implementation will be phased (on a Ward by Ward basis) within six months of completion of each Ward within the Programme.

Agreed Management Action(s)

The processes (designed and implemented above) will include a monitoring arrangement, with quarterly checks made to confirm the completeness and accuracy of the inventory in Confirm.

With this action being inextricably linked with the ongoing Energy Efficient Street Lighting Programme, implementation will be phased (on a Ward by Ward basis) within six months of completion of each Ward within the Programme, with full completion by 30 June 2022.

It has been agreed with Internal Audit that an implementation date of 20 December 2019 has been agreed with Internal Audit, enabling them to perform sample testing across the wards that have been completed at that time.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: 20 December 2019

3. Recommendation – Electric Testing Ltd Testing Results

Electrical Testing Ltd (ETL) should be requested to establish a single data source that can be accessed by the Council to access both historic and current electrical testing results.

Agreed Management Action(s)

Street Lighting Maintenance Team will contact Electrical Testing Ltd (ETL) to:

- determine whether the ETL database can be imported to Confirm; or
- request access to a single database for the retrieval of all test results.

If this cannot be achieved, management will accept the risk of inaccuracy associated with reconciling completed testing with outstanding testing across a number of separate databases.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: 31 March 2019.

3. Street Lighting and Traffic Signals: Process and quality assurance documentation and training

Low

Our review established that there are no documented processes and procedures supporting both street lighting and traffic signals operation and maintenance.

Additionally, specific street lighting and traffic signal operation and maintenance training is not provided for new team members. Instead, standard Council induction training is provided for new employees and specific street lighting and traffic signal training is delivered via work shadowing and 'on the job' experience.

Risk

- Street lighting and traffic signal operation, maintenance and quality assurance procedures are not consistently applied; and
- The standard of training delivered to new employees is not consistent.

1. Recommendation – Operation and maintenance procedures

Standard street lighting and traffic signal operation and maintenance procedures should be designed and implemented, and a regular ongoing review process established to ensure that procedures remain aligned with applicable regulatory requirements and any operational changes.

Agreed Management Action(s)

Street Lighting and Traffic Signals Operational Guides will be developed, implemented, and reviewed to ensure that processes align with current regulatory requirements.

Operational Guides will be implemented within six months of implementation of the Roads Improvement Plan, or by 30 September 2019, whichever comes first.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: 30 September 2019

2. Recommendation – Refresher training for existing employees

Street lighting and traffic signal operation and maintenance refresher training based on the content of the new procedures should be designed and delivered to all new and existing employees.

Agreed Management Action(s)

An essential Learning Matrix that specifies the refresher training that the team requires to complete on an ongoing basis has been developed and provided to Learning and Organisational Development for their review and feedback, with no response received as yet.

The matrix will now be implemented and employee training requirements will be assessed (and agreed) as part of the Annual Conversations.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: 20 December 2019

4. Traffic Signals: Evidence of pre installation design and acceptance testing	Low

Our review confirmed that since moving to a paperless system, the Traffic Signals Team no longer document completion of the first person testing and independent second person review of unit design and factory and site acceptance testing performed prior to installation of new, or upgrades to existing traffic signals. Management has advised that testing is still performed, but is no longer documented.

Previously, a project checklist was completed detailing the testing performed on all new or upgraded traffic signals; who had completed both the initial testing and independent review; and the testing outcomes.

Risk

- Issues with traffic signal performance cannot be compared to the outcomes of pre installation testing performed; and
- The quality of testing performed cannot be assessed or potential areas for training identified.

1. Recommendation – Paperless testing checklist

A paperless checklist should be established; retained on InView; and mapped to the relevant traffic signal on for future reference, ensuring that the outcomes of first and second level testing performed prior to installation of all new/upgraded traffic signals is recorded and maintained. This document should also include details of the engineers who have performed the relevant testing steps.

Agreed Management Action(s)

A checklist will be introduced to record all factory and site acceptance testing and uploaded onto InView against the appropriate asset. The checklist will record engineer acceptance and review.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: By 31 March 2020.

2. Recommendation – Guidance supporting testing checklist

The revised checklist should be circulated to all team members with guidance on how it should be completed and retained;

Agreed Management Action(s)

Workshop to be arranged to guide all relevant team members on the processes for completion and retention of the checklist.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: By 31 December 2019.

3. Recommendation – Checklist retention procedures

The requirement to complete and upload the checklist should be in included in the operational procedure documentation noted in Finding 3, management action 1 in this report.

Agreed Management Action(s)

Processes for the completion and retention of the checklist to be included in appropriate Operational Guide.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure; Alan Simpson, Street Lighting and Traffic Signals Maintenance Manager; Robert Mansell; Tony Booth; and Lindsey McPhillips.

Implementation Date: 31 March 2020.

5. Traffic Signals: Supplier management framework	Low

Monthly supplier management meetings have not been held with Siemens since February 2018 to monitor progress with annual electrical testing.

Management has advised that the traffic signals maintenance contract with Siemens expires 31st October 2018 and new contract is currently being procured.

Risk

- Issues or queries in relation to ongoing traffic signal maintenance and annual electrical testing have not been escalated to and discussed with Siemens; and
- Penalties for poor performance may not have been applied.

1. Recommendation – Supplier performance meetings

Monthly supplier performance meetings should be reinstated, and supported by a clear agenda, with actions documented and their implementation progress tracked at subsequent meetings.

Agreed Management Action(s)

Monthly meetings (with a clear Agenda) with supplier will be reinstated and will be included in any subsequent Contracts.

Minutes of Monthly Meetings recorded (filed on shared drive), with “actions” reviewed at subsequent meetings (and carried over (if necessary)).

Owner: Paul Lawrence, Executive Director of Place

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager, Transport Infrastructure

Implementation Date: By 31 March 2019.

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on 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 or brand 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 or brand 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 or brand of the organisation.
Low	A finding that could have a: • ***Minor*** impact on the organisation's 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.

Appendix 6

The City of Edinburgh Council
Internal Audit

Validation of Internal Audit Implemented and Sustained Management Actions

Final Report

9 April 2019

CW1810

Overall report rating:

Significant enhancements required	Significant areas of weakness and non-compliance in the control environment and governance and risk management framework that puts the achievement of organisational objectives at risk

•EDINBVRGH•
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018. 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

Internal Audit (IA) findings are raised where audit outcomes confirm that the controls established to mitigate the Council's most significant risks are either inadequately designed or are not operating effectively.

When finalising IA reports, management agree to implement agreed actions that will address the control weaknesses identified. Implementation of these agreed actions will ensure that the associated risks are effectively managed, reducing the Council's overall exposure to risk.

It is essential that (once implemented), the control improvements are effectively sustained. If not, the Council remains exposed to an unnecessary level of risk.

A 'validation' audit was introduced in the 2018/19 IA plan to assess whether management actions implemented to address historic findings raised by IA have been sustained and remain effective.

In March 2018, a 'self-attestation' exercise was completed across the Council. This involved Executive Directors attesting whether all 174 IA findings (48 High and 126 Medium) raised in the period 1 April 2015 to 31 March 2017 had been implemented and sustained; implemented but not sustained; or not implemented (see Appendix 2 for definitions).

The Executive Directors confirmed that a total of 114 (30 High and 84 Medium) IA findings raised had been implemented and sustained.

Scope

The objective of this review was to validate whether a representative sample (10%) of the 114 High and Medium rated IA findings have been effectively implemented and sustained as confirmed by completion of the 'self-attestation' exercise.

Of the 114 findings, a sample of 11 findings with 24 supporting management actions covering all Council Directorates was selected, and tested, to confirm their current status.

Our review concluded as at 7 December 2018, and our findings and opinion are based on the outcomes of our testing at that date.

Where the necessary control improvements have not been implemented and effectively sustained, the relevant findings and supporting management actions have been reopened; regraded (where appropriate based on residual risk) and reported as overdue, based on the originally agreed implementation dates.

2. Executive summary

Total number of findings: 3

Summary of findings reopened	
High	1. Communities and Families - Use of unsupported technology devices in schools
High	2. Health and Social Care – Management structure and business support arrangements – regraded from Medium
Low	3. Resources - One Time Payments Authorisation – regraded from Medium

Opinion

In our opinion, significant enhancements are required to ensure that management effectively implement and sustain the necessary control improvements to support closure of Internal Audit findings.

Our review confirmed that control improvements supporting 8 of the 11 original findings (4 High and 4 Medium) had had been effectively implemented and sustained, with three findings (1 High, and 2 Medium) where further action is required to fully address the risks.

Consequently, these findings and supporting management actions that have not been fully implemented and sustained have been regraded (where appropriate reflecting the associated residual risk); will be reopened; and reported as overdue based on originally agreed implementation dates.

One finding has been reopened as a High; one regraded from a Medium to a High; and one finding downgraded from Medium to Low.

Details of our ratings classifications and an explanation of the conclusions applied to our validation outcomes are included at Appendices 1 and 2.

Communities and Families - Use of unsupported technology devices in schools

The first reopened High rated finding relates to use of unsupported technology devices in schools. The original finding included three agreed management actions. Of these, one has been implemented but not sustained; one partially implemented; and one not implemented. The rating for this finding has not been reduced as the residual risk associated with lack of confirmation that non-centrally supported devices that could contain personal, sensitive information are appropriately secured is considered significant.

Health and Social Care – Management structure and business support arrangements

The second reopened High finding (regraded from Medium) relates to lack of clarity in relation to the Partnership' management structure, and the scope and oversight of business support arrangements provided by the Council to the Health and Social Care Partnership. The original finding included three management actions, and none of these have yet been implemented.

This is partially attributable to a significant number of senior management changes within the Partnership (the new Chief Officer was appointed in May 2018) and the Council (the new Head of Customer, with responsibility for Business Support functions, except in Schools, was appointed in March 2017). It is also important to note that the Business Support structure was only established in October 2016 as part of the Council's Transformation Programme, following a simplistic approach to the centralisation of the majority of staff with Business Support job titles into a single function, with significant additional time required for its subsequent implementation.

As the full population of Partnership operational processes has not been documented (this is reflected in the High rated finding raised in the Health and Social Care Partnership Purchasing Budget Management review, completed July 2018), it has not been possible to reach formal agreement on the scope of the services provided by the Business Support and Transaction teams within Customer to support the Partnership, or establish appropriate service levels and supporting key performance indicators enabling effective oversight of service delivery.

The control gaps and residual risks associated with lack of clear definition and oversight of Partnership business support arrangements provided by the Council have been highlighted in the significant findings raised in relation to Business Support administrative support services provided to care homes (Care Homes Assurance review, February 2018); management of client funds (Social Work Centre Bank Account Reconciliations review, April 2018); and a number of financial and operational processes (Health and Social Care Partnership Purchasing Budget Management review, July 2018).

Resources - One Time Payments Authorisation

The final Low rated finding (regraded from Medium) relates to controls supporting authorisation of manually processed ‘one time’ payments. The original finding included three management actions. Of these, two have been implemented and sustained, and one partially implemented and sustained. The reduced rating reflects the residual risk associated with processing lower volumes of payments, without confirming that they have all been appropriately authorised by Directorates/Divisions.

Overall conclusion

Consequently, all three Findings have been reopened and will be reported as overdue based on originally agreed implementation dates.

Our detailed findings and new recommendations are detailed at Section 3 below.

3. Detailed findings

1. Communities and Families - use of unsupported technology devices in schools	High

Original finding

This High rated finding was originally raised in the Schools IT Systems review completed in February 2016. The original finding established that:

- Teaching staff commonly use personal and school-managed computers for work purposes, which may on occasion involve personal and sensitive data. These devices are not hosted on behalf of the Council by CGI, and may not have full security such as passwords and anti-virus and encryption software installed. We identified one instance where sensitive personnel data was held on an unencrypted memory stick;
- Office 365 has been introduced to all schools, enabling staff and pupils to work remotely on a secure web-based platform, eliminating the need for data to be stored on hard drives. However, use of Office 365 is still limited in some schools and there is evidence that data is still stored on personal and school-managed hard drives;
- Whilst staff are required to comply with the corporate Acceptable Use of IT policy, the policy does not specify security required when staff are using their own device for work purposes; and
- We further noted that staff at six of the14 schools visited had not completed mandatory training on information governance at time of our audit visits between September and November 2015.

Validation outcomes

The outcomes of our validation work confirmed that one of the three management actions associated with this finding has been implemented but not sustained; one partially implemented and sustained; and one not implemented.

Consequently, this finding will be reopened as a High rated finding (reflecting the residual risk) with supporting management actions tracked against the originally agreed implementation dates.

Our testing established that:

- Guidance for the use of non-hosted devices (now referred to as Personal Devices and Office 365) has been created, however there is a lack of clarity in the guidance in relation to physical security of personal devices containing Council information.

  Conclusion: Partially implemented and sustained.
- Evidence was provided confirming that guidance had been introduced to schools via head teachers' and ICT co-ordinators' forums, and that it had been circulated once to schools.

  Conclusion: Implemented but not sustained.
- An email was received confirming that annual confirmation that employees are applying the guidance is not obtained.

  Conclusion: Not implemented.

Risk

The original risk that personal and sensitive data may be held on unencrypted devices, increasing the risk of a data security breach if the device is lost or stolen has not been fully mitigated, as confirmation that employees are applying the guidance when using personal and school equipment is not obtained.

1. Recommendation – Guidance for use of non-hosted devices

The guidance for use of non-hosted devices in schools should be expanded to include physical security of devices (i.e. safe storage); and should be re-issued annually across all schools; special schools; and nurseries.

Agreed Management Action

A new protocol has been developed to accompany the Acceptable Use Policy

This will be emailed to all school offices in May ready for the new school year.

Owner: Alistair Gaw, Executive Director of Children and Families

Contributors: Andy Gray, Head of Schools and Lifelong Learning**,** Cheryl Buchanan, Operations Manager; Lorna Sweeney, Senior Manager Quality, Improvement & Curriculum; Richard Burgess, ICT Strategy Manager

Original Implementation Date: 31 March 2016

Revised Implementation Date: 30 August 2019

2. Recommendation – Application of guidance by employees

Employees should be requested to provide annual confirmation that they have read and understood the guidance, and consistently applying it to all devices used in schools.

Agreed Management Action

Staff will be asked to read and sign annually that they will adhere to the guidance, particularly the use of passwords and minimum operating requirements.

Owner: Alistair Gaw, Executive Director of Children and Families

Contributors: Andy Gray, Head of Schools and Lifelong Learning, Cheryl Buchanan, Operations Manager; Lorna Sweeney, Senior Manager Quality, Improvement & Curriculum; Richard Burgess, ICT Strategy Manager

Original Implementation Date: 31 March 2016

Revised Implementation Date: 30 August 2019

2. Health and Social Care – Management structure and business support arrangements	High

Original finding

This Medium rated finding was originally raised in the Integrated Health and Social Care review completed in August 2015 and established that:

Although responsible officers had been assigned from both NHS Lothian and CEC to support several Partnership and EIJB processes, it is not clear how, roles and responsibilities will split between the two parties. This includes, but is not limited to, how the skills and resources of both partners will be used effectively to meet the demands for Health and Social care appropriately.

Staff who support both delegated Partnership functions and the EIJB are employed either by CEC or NHS Lothian, and this will continue to be the case following delegation.

An integrated partnership and EIJB management structure has not yet been agreed, and this may take a significant amount of time to implement once the structure has been agreed.

Functions which are not delegated, for example business support roles, will be managed separately by the Council and NHSL. The operation of these functions will need to be agreed by both bodies, and the two must work co-operatively to agree how best to support the Partnership and IJB. This will be made more difficult by the changes in management as internal secondments finish, and as the new management structure begins, therefore potentially losing continuity between the pre- and post-delegation management structures.

Validation outcomes

The outcomes of our validation work confirmed that none of the three management actions associated with this finding have been implemented.

Consequently, this finding will be reopened as a High rated finding (reflecting the residual risk) with supporting management actions tracked against the originally agreed implementation dates.

Our testing established that:

- The originally agreed management action to implement an agreed Partnership organisational management structure has not been finalised, implemented, and embedded due to a number of Senior Management and Chief Officer changes within the Partnership and the Council.

  Conclusion: Not implemented

- The originally agreed management action to arrange focus groups to discuss partnership and EIJB business support arrangements and establish options has not been completed.

  Management has advised that the requirement for focus groups was superseded by meetings between the Interim Chief Officer and Head of Customer and Digital Services. Dates from two meetings in March and April 2018 were provided as evidence that these meetings took place, however no evidence of meeting outcomes; decisions in relation to the agreed structure of business support arrangements; and dates of subsequent meetings was provided.

  Conclusion: Not implemented

- The originally agreed management action to establish SLAs for business support outwith the organisational management structure has not been completed.

  Conclusion: Not implemented

Risk

- Partnership senior management structures are unclear and the Partnership may not be consistently and effectively managed; and
- The Partnership may not receive either the required scale or quality of operational business support required to ensure effective service delivery.

1. Recommendation – Partnership Management Structure

Review of the Partnership operational management structure should be completed by the Chief Officer, approved by the EIJB, and implemented.

Agreed Management Action

The Partnership's organisational management structure will be finalised, implemented, and embedded.

The revised structure does not need to be approved by the IJB because it is an operational matter. It will however be presented to the EIJB for information.

The revised implementation date of April 2020 will allow completion of Partnership budget and transformation Programmes.

Owner: Judith Proctor, Chief Officer HSCP

Contributors: Cathy Wilson, Health and Social Care Partnership Operations Manager

Original Implementation Date: 31 December 2015

Revised Implementation Date: 30 April 2020

2. Recommendation – Business Support Arrangements

Business support arrangements for both the Partnership and EIJB should be agreed, implemented, and consistently applied.

Agreed Management Action

- Focus Groups to review and discuss current Partnership and EIJB business support arrangements will be established.
- Senior Partnership Managers will nominate a Partnership Officer aligned to a business support service to provide insight on role expectations and key statutory and non-statutory functions for each business support function.
- Business Support Senior Managers will also nominate relevant officers to participate in Focus Groups.

Owner: Judith Proctor, Chief Officer HSCP

Contributors: Stephen Moir, Executive Director of Resources**;** Nicola Harvey, Head of Customer and Digital Services; John Arthur, Senior Manager, Business Support; Cathy Wilson, Health and Social Care Partnership Operations Manager

Original Implementation Date: 31 December 2015

Revised Implementation Date: 30 June 2019

3. Recommendation – Business Support Service Level Agreements

- A proportionate set of business support service level agreements and support key performance indicators that cover all aspects of business support and transaction services provided to the Partnership by the Council should be defined; approved by both Partnership and Council senior management; and implemented; and
- Ongoing meetings should be established between relevant senior managers in the Partnership and Business Support to ensure performance against SLAs is monitored on an ongoing basis, with any performance issues escalated to the Partnership senior management team for consideration and resolution.

Agreed Management Action

- The Partnership and Business Support Service will jointly establish SLAs for business support outwith the organisational management structure.
- Regular meetings between relevant senior managers in the Partnership and Business Support will be established to ensure performance against SLAs is monitored. Any performance issues will be escalated to the Partnership's Executive Team for consideration and resolution.

Owner: Judith Proctor, Chief Officer HSCP

Contributors: Stephen Moir, Executive Director of Resources**;** Nicola Harvey, Head of Customer and Digital Services; John Arthur, Senior Manager, Business Support; Cathy Wilson, Health and Social Care Partnership Operations Manager

Original Implementation Date: 31 December 2015

Revised Implementation Date: 31 October 2019

3. Resources - One Time Payments Authorisation — Low

Original finding

This finding was originally raised as a Medium in the Continuous Controls – One Time Payments review completed in January 2016, and established that:

- There were no effective controls around authorisation and approval of 'One Time Payment' (OTP) payments.
- The Oracle payment system did not record the name of the relevant Service Area manager who authorised the payment. Instead, a paper form, requiring two authorising signatures, was provided by the relevant service area to the Payments Services Team;
- Some payment request forms are 'pp'd' by a member of staff within the authorisation field.
- Some signatures authorising payment were illegible;
- Payments were processed by the Payments Services Team on the basis that they had been appropriately authorised by the service area. There was no authorised signatory list or delegated authority level available for reference by the for the Payments Services team to confirm that authorisation received from service areas is appropriate and authentic; and
- Segregation of duties controls supporting processing of OTPs were not effective.

Validation outcomes

The outcomes of our validation work confirmed that 2 of the 3 management actions associated with this finding have been implemented and sustained, and 1 has been partially implemented.

We also established that the volume of one time payments had reduced by approximately 2,000 and £1.3m in value between June 2016 and August 2017, reducing the risks associated with manual authorisation and processing.

Consequently, this finding will be reopened and downgraded to a Low rated finding (reflecting the residual risk) with supporting management action tracked against the originally agreed implementation dates.

Our testing established that:

- Payment Services agreed that any one time payment forms received with a 'pp' in the authorisation field would be rejected. Review of a sample of 25 one time payments established that only one payment request had been processed that included a 'pp' in the authorisation field, however Payments Services confirmed that the supporting documentation had been approved by the correct person in the service area; that the processing of this application had been an error and that the normal process is to reject these applications.

  Conclusion: Implemented and sustained.
- Payment Services had agreed that they would request one time payment authority lists from service areas; check all requests prior to processing to ensure that the appropriate authority had been obtained; and reject any requests that have not been correctly authorised. This management action has been partially completed.

  Review of a sample of 25 payments confirmed that 18 had been compared to an approved list of authorisers prior to payment, whilst 7 had not. Supporting evidence was provided for 6 of the 7 payments.

Management has confirmed that a list of authorisers is maintained for services areas who submit high volumes of one time payment requests (for example Council tax, PPSL, and Parking) and effective checks are performed to confirm that these have been appropriately authorised prior to processing the payment. Payments that have not been appropriately authorised are rejected.

Authorisation lists are not maintained for service areas that submit ad hoc one time payment requests, therefore no authorisation checks are performed prior to processing. If supporting evidence is not provided for a payment, the request will be rejected and returned.

Conclusion: Partially implemented and sustained

- Payment Services also agreed that manual signatures on payment authorisation forms would be replaced by requests received via e mail; processed where addresses were consistent with agreed departmental approval lists; and e mail requests retained in archive folders to enable confirmation of ongoing process compliance and audit review.

Review of the payment authorisation process established that whilst paper payment requests continue to be accepted, the e mail confirmation process has been introduced. E mail payment requests retained for 12 months prior to automatic deletion by CGI, however all payment request forms are printed and archived at Iron Mountain in accordance with the Council’s records retention policy.

Conclusion: Implemented and sustained.

Risk

Potential risk of fraud and / or error associated with low volume high value payments where appropriateness of service area payment authorisation is not confirmed.

1. Recommendation – Authorisation of payment requests

- For ad hoc payment requests, a risk based approach should be adopted, where Divisions will be contacted to confirm that authority for all one time payments in excess of a specified threshold is appropriate; and
- Payments that have not been appropriately authorised should be rejected.

Agreed Management Action

- Services will be contacted and requested to confirm appropriateness of authority for all ad hoc payment requests received in excess of £500;
- Payments that have not been appropriately authorised will be rejected;
- A revised process note will be prepared and implemented within the Payments team, and signed confirmation obtained from team members that they understand the reviewed process; and
- A small sample of ad hoc payments will be reviewed by Payments managers on an ongoing basis to confirm that the process has been effectively embedded.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey, Head of Customer and Digital Services; Neil Jamieson, Senior Manager, Customer Contact and Transactions; Sheila Haig, Customer Manager.

Original Implementation Date: 29 February 2016

Revised Implementation Date: 30 April 2019

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on 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 or brand 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 or brand 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 or brand of the organisation.
Low	A finding that could have a: • ***Minor*** impact on the organisation's 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.

Appendix 2 – Conclusion definitions

Conclusion	Definition
Implemented and sustained	Controls have been fully implemented, and our testing confirmed that they have been sustained
Partially implemented and sustained	Controls have been partially implemented, and our testing confirmed that the elements implemented have been sustained
Implemented but not sustained	Controls were initially implemented, but have not been sustained
Not implemented	Controls have not been implemented

Appendix 7

The City of Edinburgh Council

Internal Audit

Place Directorate

Port Facility Security Plan

Final Report

01 April 2019

PL1809

Overall report rating:

Adequate	An adequate and appropriate control environment and governance and risk management framework is in place enabling the risks to achieving organisation objectives to be managed

·EDINBVRGH·
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk, and Best Value Committee in March 2018. 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 City of Edinburgh Council (the Council) owns, manages, and maintains the Hawes Pier (the Pier) port facility in South Queensferry. The Pier is a 300m long gradual slipway facility with security fencing and a double gate which is situated at the head of the pier. Security at port facilities in the UK is governed by legislation and guidance including the Ship and Port Facility Security Regulations (2004), and is subject to oversight by the Maritime Security & Resilience Division of the UK Department for Transport (DfT).

As owner of the Pier, the Council is responsible for ensuring an appropriate Port Facility Security Plan (PFSP) is in place, and that security arrangements are consistently and effectively applied in line with DfT requirements. The PFSP for Hawes Pier is a c.40-page document (classified as OFFICIAL-SENSITIVE), prepared and maintained by the Council using a standard DfT template, and outlines the range of security measures and requirements which the DfT expect to apply at the Pier when cruise ships visit. It is subject to annual review and approval by the DfT, who have the authority to undertake planned or unannounced visits / inspections as they consider appropriate. An annual independent audit of the PFSP (for example, by the relevant local authority Internal Audit team) is also required.

One of the key PFSP requirements is a designated Port Facility Security Officer (PFSO) – a Council employee who has responsibility for managing and overseeing security arrangements at the Pier, principally on the days when cruise ships are visiting. Operational duties of port security are outsourced to a third-party supplier, Profile Security, who report to the PFSO. Management has advised that this arrangement has recently been re-procured.

The cruise ship season is principally from May to September, and in 2018 a total of 22 cruise ships used the Pier, generating net income (after direct costs) of c.£350K. Visits usually last one day but occasionally involve anchoring overnight.

In addition to cruise ships, the Pier is used by:

- Visiting cruise ships to ferry passengers on and offshore via tender (these larger cruise ships are unable to dock directly at Leith or Rosyth due to their size);
- Leisure boat firms who operate from offices on the Pier and provide a range of short cruises (principally from April to October);
- The Royal National Lifeboat Institution (RNLI) operates a lifeboat station from buildings on the Pier;
- Targe Towing operates towing boats (tugs);
- South Queensferry Coastguard;
- INEOS has a small office and storage facility on the pier and transfers personnel and equipment to the nearby Hound Point oil terminal (INEOS sub-contractors also use the pier); and
- Members of the public / water sport enthusiasts also use the pier.

Some third-party users of the Pier (for example, Targe and INEOS) implement their own security measures throughout the year, however during a ship visit they must comply with the security procedures outlined in the PFSP.

The presence of a cruise ship in the Firth of Forth presents an increased risk of a security incident. Consequently, on the day of each ship's visit, a Temporary Restricted Area (TRA) is set-up around the Pier. All visitors wishing to access the Pier must be issued with a temporary day pass by security staff.

daily record is taken of visitors’ names; the unique serial number of each temporary pass issued; the visitor's organisation; the reason for access; and the times in and out. Similarly, security staff are required to perform visitor (bag and person) and vehicle searches for those entering the restricted area, but not boarding the ship (such as tourist information staff, delivery drivers or maintenance workers).

During a ship visit, security staff perform and maintain a record of hourly patrols of the TRA and are responsible for escalating any issues to the PFSO (who will be onsite) and take appropriate action. In the event of a major incident, the PFSO is responsible for contacting the emergency services and liaising with the visiting ship, which will initiate its own evacuation process in conjunction with the Pier’s, where appropriate.

All visiting ships are required to complete a Declaration of Security which is reviewed and approved by the PFSO. This is an official document which outlines the details of the ship visit, and the responsibilities and accountabilities of both parties for the duration of the visit. The ship must also provide a list of names of persons wishing to disembark or board the ship at the Pier, which security staff reference when manning the gates.

Scope

The scope of this review was to assess whether the PFSP has been consistently applied throughout the season. Our review was completed on 28 January 2019, and our opinion and findings are based on the outcomes of our work as at that date.

Due to the timing of the audit being outwith the cruise ship visiting period (May to September), it was not possible to carry out a site visit. Consequently, a retrospective desk based review of security documentation for a sample of cruise ship visits was performed.

2. Executive summary

Total number of findings: 2

Summary of findings raised	
Medium	1. Non-compliance with DfT requirements
Low	2. Resilience and Risk Management

Opinion

Review of the documentation retained to support evidence of compliance with the DfT approved Port Facility Security Plan during the 2018 cruise ship season has confirmed that security controls applied were adequate, with some moderate instances of non-compliance with DfT requirements evident, and areas for improvement identified.

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

The first finding highlights the areas of non-compliance with the DfT requirements outlined in the Port Facility Security Plan, while the second highlights opportunities to improve the risk management; contingency planning; and evacuation processes necessary to support the secure operation of the Pier and confirm that potential threats and incidents have been identified and can be effectively managed.

It is acknowledged that the PFSO post was filled in May 2018; however, while awaiting security clearance, the PFSO shadowed the Depute PFSO and did not independently oversee security arrangements until almost the end of the cruise ship season (circa September 2018).

Following the successful procurement of Profile Security on 13 December 2018 to deliver the ongoing operational aspects of Pier security arrangements on behalf of the Council, all findings raised in previous Internal Audit reviews have now been addressed and closed

Our detailed findings and recommendations are laid out within Section 3: Detailed Findings

3. Detailed findings

1. Non-compliance with DfT requirements — Medium

The Port Facility Security Officer (PFSO) is responsible for ensuring that security operations are compliant with Department for Transport (DfT) requirements throughout the shipping season by consistently applying the PFSP for all cruise ship visits.

Our retrospective review of security documents for a sample of cruise ship visits selected from the from the 2018 shipping schedule identified the following areas where available documentation was not sufficient to confirm that DfT security requirements had been met:

- **Initial Comprehensive Port Facility Security Survey:**

  Section 3, Part A, Sub-section 20 of the Port Facility Security Plan (PFSP) states that it is the responsibility of the PFSO to conduct an initial comprehensive security survey of the port facility, taking into account the relevant Port Facility Security Assessment (PFSA). The PFSA is undertaken by DfT with input from the PFSO and other relevant port facility staff. It assesses the assets and risk of threats and vulnerabilities associated with the Pier, and is valid for 5 years.

  At the time of our review, the PFSO could not provide supporting evidence to confirm that the initial comprehensive security survey had been completed,

- **PFSO Pier Inspections:**

  Section 3, Part A, Sub-section 3 of the PFSP states that the PFSO is responsible for conducting inspections of the Pier on the day prior to the ship's arrival, and before the TRA is set up on the day of the visit. Whilst evidence was available to support completion of searches on the day of arrival, there was no documentation to support completion of searches on the day prior to arrival for 6 of 22 cruise ships that visited during the 2018 season.

- **Recording of Visitor Identification:**

  It is a DfT requirement that photographic identification (Valid Driving Licence or Passport) must be provided by visitors upon being issued a temporary day pass. Security are required to check and retain visitor identification until the visitor returns the pass when leaving the TRA.

  Documentation detailing checks performed on a sample of 8 visitors across 3 days when a ship was present at the Pier was reviewed to confirm whether the correct procedures were being applied by security staff. This confirmed that whilst visitors' details are recorded, no record of the identification provided is retained; and no log is maintained to confirm that identification has been checked; retained; and returned. The PFSO has confirmed that this procedure is applied in practice.

- **Unmoderated Number of Visitor Searches:**

  Section 3, Part A, Sub-section 11 of the PFSP states that while the Pier is at a Security Level 1, the "minimum percentage" of visitors, as stated by DfT, should be searched by security staff. Management clarified that security staff do not understand how to apply this procedure, and instead search all visitors with bags, and a sample of visitors with no bags.

  A sample of visitor search documentation was selected for 8 days when a ship was present at the Pier, and reviewed to determine the percentage of daily visitor searches performed, based on the number of temporary day passes issued. This confirmed that search frequency was generally adequate (4/8 days = 64-71%; 2/8 days > 40%).

However, as the process used in practice for selecting the sample of visitors to be searched is not documented, it cannot be assumed that the frequency of searches performed remains appropriate for all cruise ship visits.

Risk

- Potential penalties and reputational damage if non-compliance with PFSP requirements is identified by the Department for Transport (DfT);
- Potential Council liability for loss of visitor identification; and
- Unauthorised persons could access the Pier or prohibited items could be passed through security.

1.1 Initial security survey

1. The Department for Transport (DfT); should be engaged to clarify the requirement to complete the "initial comprehensive security survey", and confirm DfT expectations in relation to the scope of the survey and documentation to be retained to support completion;
2. The survey should then be completed and recorded in line with DfT requirements; and
3. If the DfT confirms that the initial security survey is not required, then this should be removed from the Port Facility Security Plan.

Agreed Management Action

A Port Facility Security Assessment (PFSA) was performed by the Department for Transport (DfT) in 2014, and remains valid. A new PFSA which will cover the next 5 years is scheduled for completion by the DfT in April 2019.

Since the audit fieldwork, we have contacted the DfT to confirm the initial comprehensive security survey requirements based on the PFSA for Hawes Pier.

A file containing documentation supporting completion of the comprehensive security survey has now been located, and details will be provided to Internal Audit.

Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager; Chris Spence, Port Facility Security Officer; Gordon McOmish, Senior Engineer, Flood Prevention.	**Implementation Date:** 31/05/19 **Date for completion of IA validation:** 17/05/2019

1.2 Pier inspections on the day prior to establishing the temporary restricted area (TRA)

1. The Department for Transport (DfT) should be engaged to explain the challenges associated with completing pier inspections on the days prior to establishing TRAs as detailed in the Port Facility Security Plan (PFSP) (Section 3, Part A: Mandatory Security Requirements, Part 3: Temporary Restricted Areas), and confirm whether the DfT require these checks to be performed;
2. If required, inspections should be performed on all days prior to establishing the TRA and recorded with supporting evidence of completion of the inspection retained; and
3. If the inspections are not required, amend the PFSP to reflect that inspections are not appropriate as the Pier remains open to the public until immediately before a ship’s arrival.

Agreed Management Action

Since the audit fieldwork, we have contacted the Department for Transport (DfT) to confirm specific inspection requirements in relation to Hawes Pier. On this basis we have updated documentation and inspection sheets, and these are now available for IA to review.

Owner: Paul Lawrence, Executive Director of Place	**Implementation Date:** 31/05/19

Contributors: Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager; Chris Spence, Port Facility Security Officer; Gordon McOmish, Senior Engineer, Flood Prevention.	**Date for completion of IA validation:** 17/05/2019

1.3 Visitor identification

A documented procedure for collecting; recording; and returning all visitor identification should be designed and implemented. This should include (but not be restricted to) obtaining a signature upon receipt from security staff; and a signature upon return by the visitor.

Agreed Management Action

We will amend visitor sheets to include type of ID used and obtain a signature upon both receipt and return of identification to the visitor.

Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager; Chris Spence, Port Facility Security Officer; Gordon McOmish, Senior Engineer, Flood Prevention.	**Implementation Date:** 31/05/19 **Date for completion of IA validation:** 17/05/2019

1.4 Visitor Searches

1. The Department for Transport (DfT) should be contacted to clarify whether current search procedures meet their requirements in relation to the minimum search percentage at Security Level 1;
2. Existing search procedures should be updated to reflect the required number of searches required to meet DfT requirements; and
3. The procedure should be communicated to security staff prior to implementation to ensure that they are aware of the number of searches to be performed.

Agreed Management Action

We have contacted the Department for Transport (DfT) to confirm specific requirements in relation to Hawes Pier. We currently ask for 100% of passengers for their shipping card which is above the DfT requirement of 35%. We will update our procedure to reflect DfT requirements, and specify our own search requirements.

Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager; Chris Spence, Port Facility Security Officer; Gordon McOmish, Senior Engineer, Flood Prevention.	**Implementation Date:** 31/05/19 **Date for completion of IA validation:** 17/05/2019

2. Resilience and Risk Management	Low

Pier Risk Register

Management has advised that the high level risks associated with operation of the Pier are included in the Transport Infrastructure risk register, however, there is currently no specific risk register and supporting risk assessments for the Pier that details the full range of risks (including, for example, security and health and safety) that apply to ongoing Pier operations.

Contingency Plans

Section 3, Part A, Sub-section 13 of the PFSP describes contingency plans for various threats to the Pier.

Whilst these plans are based on the DfT-prescribed plan template and have been adequately populated, our review established that the threats and associated contingencies included in the plan (the threat of a bomb or explosion) are limited and do not cover the full range of potential risks and threats to pier security.

Evacuation Procedures

The PFSP does state that in the event of a major incident, an evacuation procedure would be initiated; however, there is no currently no comprehensive evacuation plan detailing roles, responsibilities, communication, and no evidence that evacuation procedures have been tested to confirm that the process can be safely and effectively performed in the event of an emergency.

Risk

- Wider risks and threats to pier security and resilience are not identified and managed; or appropriate contingency plans established;
- Security staff; visiting ships; and third parties are unaware of their roles and responsibilities in the event of an evacuation, with a potential risk to public safety; and
- Reputational risk if incidents are not effectively managed.

2.1 Risk Register

1. A risk register should be developed; implemented; and consistently maintained that details all potential risks (including security risks) that could impact upon the operation of the pier;
2. The risk register should include reference to the relevant controls (for example security checks; contingency and evacuation plans) established to ensure that these risks are either effectively managed, or that an appropriate and timely response can be implemented; and
3. Supporting risk assessments should be performed where applicable (for example, health and safety risk assessments).

Agreed Management Action

The most appropriate risk register to record and manage the specific risks associated with the operation of Hawes Pier will be identified; and the risks will be recorded; rated; and matched to the established controls.

Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager; Chris Spence, Port Facility Security Officer; Gordon McOmish, Senior Engineer, Flood Prevention.	**Implementation Date:** 31/05/19 **Date for completion of IA validation:** 17/05/2019

2.2 Contingency Plans and Evacuation Procedures

1. An assessment should be performed to establish whether the existing Pier contingency plan that includes alternative operational processes in the event of a bomb threat or explosion is an appropriate response and can be applied if any other risks or threats (recorded in the risk register as per agreed management action 2.1) to Pier security crystallise;
2. Where the existing contingency plan is not considered appropriate; alternative contingency arrangements should be established; agreed; and communicated to all users of the Pier;
3. A comprehensive evacuation plan to be used in the event of a major incident should be developed and implemented. It should include (but not be restricted to) roles and responsibilities of the Port

Facility Security Officer (PFSO) and security staff; liaison with the Emergency Services; communication with the ship and visitors; and evacuation routes and assembly points. This plan should be developed in advance of the planned Department for Transport (DfT) evacuation exercise in scheduled for June 2019.

4. The evacuation plan should be communicated to all users of the Pier, including third parties; and
5. The evacuation plan should be tested at least every 18 months as per applicable DfT requirements, with the outcomes documented, and lessons learned incorporated into the plan and future evacuation exercises.

Agreed Management Action

Beyond a certain threat level, the Council's Resilience team and public safety partners (for example the Police) assume responsibility for implementation of emergency and contingency plans.

The Port Facility Security Plan (PFSP) will be updated to reflect the extent of the Port Facility Security Officer's (PFSO) responsibilities in the event of a major incident, and the contacts and escalation processes to be applied when the threat level increases beyond this to ensure that appropriate evacuation procedures are applied and contingency arrangements implemented.

A full pier evacuation exercise will be completed by the end of October 2019.

Owner: Paul Lawrence, Executive Director of Place **Contributors:** Gareth Barwell, Head of Place Management; Cliff Hutt, Service Manager; Chris Spence, Port Facility Security Officer; Gordon McOmish, Senior Engineer Flood Prevention.	**Implementation Date:** 30/11/19 **Date for completion of IA validation:** 15/11/2019

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: - ***Critical*** impact on 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 or brand 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 or brand 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 or brand of the organisation.
Low	A finding that could have a: - ***Minor*** impact on the organisation's 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.

Appendix 8

The City of Edinburgh Council
Internal Audit

Developer Contributions

Final Report

1 May 2019

Project Code
PL1802

Overall report rating:

Significant enhancements required	Significant areas of weakness and non-compliance in the control environment and governance and risk management framework that puts the achievement of organisational objectives at risk

·EDINBVRGH·
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018 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

Developer contributions (also referred to as infrastructure contributions; planning obligations; and section 75 Agreements in Scotland) are contracts entered into between a landowner or developer and the planning authority. They mostly occur in relation to planning applications, and can include financial contributions towards schools, roads, transport, public realm, and affordable housing.

Relevant legislation and guidance

The Scottish Government's Supplementary Guidance (SG16) on Developer Contributions notes that:

- Section 69 of the Local Government (Scotland) Act 1973 gives authorities the power to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of their functions. This provision enables agreements to be made which can include financial payments; and
- both Section 75 and 69 Agreements will be used by Councils to secure developer contributions. In cases where a relatively small financial contribution in relation to the overall development cost is involved, it may be possible (with developer agreement) to issue a Council invoice for developer contributions of less than £20,000. Payment of the invoice will be required before the decision notice is issued.

The City of Edinburgh Council's (The Council) LDP Supplementary Guidance - Developer contributions and infrastructure delivery also notes that:

- developer contributions (except for payments toward land) will be index linked;
- contributions towards education infrastructure will be held for 30 years from the date of construction of new school infrastructure;
- all other contributions will be held for 10 years;
- if the actual cost of delivering the new infrastructure is lower, S75 legal agreements can make provision for the repayment of unused contributions;
- applicants have the opportunity to ask the Council to consider modifying existing S75s to reflect contribution rates that have been updated to take account of up-to-date costs; and
- applicants have the statutory right to apply to the Council for the modification or discharge of a Section 75 agreement.

Identifying, calculating, and agreeing developer contributions

The Council's Planning team process all planning applications received, including assessing whether developer contributions are required.

The first step is to consider whether the planning application is aligned with the Council's Local Development Plan (LDP) which sets out a development strategy and several proposals across the city for the next 10 years, with supporting infrastructure requirements detailed in the Action Programme (AP). These can be located at Edinburgh LDP and AP.

If the development is included in the LDP and AP, a planning case officer will determine the nature and value of contributions relevant to the planning application. Where the proposed development is not included in the LDP and AP, further engagement with service areas (for example, Transport and Housing) is required to establish the infrastructure requirements; associated costs; and contributions required.

The Planning case officer then co-ordinates a proposal in conjunction with other service areas. The proposal is discussed and negotiated with the developer.

Final proposals are reviewed by planning team managers and presented to the Development Management Sub-Committee (DMSC), for approval once every 2 weeks. Some proposals, with smaller contribution amounts, are not presented to DMSC for review, and are not supported by legal agreements. Following Committee approval, proposals are referred to the Council's Legal team and outsourced to an external legal firm for development of the relevant legal agreements.

The legal agreement specifies the total value of the contribution; phasing of payments; and utilisation of the funds. Some legal agreements also state the requirement for exclusive use of contributions for a specified purpose and/or for a specified duration.

All key documents relating to each stage of the planning application, including final developer legal agreements, are publicly available on the Council's planning portal.

Two planning officers are responsible for monitoring developments across the city; reviewing development progress in their area; and liaising with developers to ensure that contributions are received on time. These planning officers also raise invoices for contributions and inform service areas when contributions have been received.

All development contributions received are administered by Finance (until funds are requested by service areas) via an excel spreadsheet that records all contributions received, and their subsequent allocation to infrastructure developments. The spreadsheet is referenced with the relevant planning application numbers, and dates back to 2003.

Treasury also allocates unutilised developer contributions into temporary investments to earn interest Income.

Planning operates under a Scottish Government Performance Framework which has target of processing every local application within 2 months from the date of application, and major development applications in 4 months or the date defined in the planning processing agreement. The Council, in conjunction with the developer, developed legal agreements for 14 major applications in 2017/18 with an average processing time of 66.2 weeks.

Scope

The objective of this review was to assess the adequacy of the design of the controls established to support development; agreement; and approval of developer contribution legal agreements by Planning and Legal Services, and subsequent administration and application of developer contributions by Finance.

The outcomes of the review also provide assurance on the controls established to manage the following risk identified in the Planning Services risk register:

Risk that section 75 developer's money is held but not used and that at a future date the developers may want the money back.

Whilst Finance manages developer contributions, there is no relevant risk recorded in the Finance risk register.

Our work was performed during the period August 2018, and concluded on 31 August 2018. Our opinion and findings are based on the review outcomes as at that date. There was a delay in issuing the draft report due to Internal Audit resourcing challenges, with the initial draft issued on 24 January 2019.

Limitations of Scope

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

- as management has confirmed that there are known weaknesses in the design of the controls supporting the end to end developer contributions process, no testing was performed to confirm how effectively the controls are applied; and
- all other aspects of Planning operations and the performance framework that do not specifically relate to developer contributions.

2. Executive summary

Total number of findings: 3

Summary of findings raised	
High	1. Backlog of legacy developer contributions
High	2. End to end developer contribution processes, procedures, and training
High	3. Ongoing management of developer contributions

Opinion

Our review confirmed that significant enhancements are required to improve the design of the controls supporting development; agreement; and approval of developer contribution legal agreements by Planning and Legal Services; and ongoing management and allocation of the funds received by Finance.

The need to enhance the design of the control framework supporting developer contributions was initially highlighted by Internal Audit in the review of Planning Controls and the Local Development Plan completed in October 2015, where 4 Medium and 2 Low rated findings were raised.

As part of the self-attestation exercise performed across the Council in February 2018, management confirmed that three of the original Medium rated actions included in this report had not been implemented. These findings reflected the need to ensure that:

1. ensure that progress against delivery of legal agreement terms is effectively monitored in the Uniform system (original implementation date: 1 January 2016);
2. review and address historic contributions totalling circa £2.3M (original implementation date: 31 January 2016); and
3. reinstate preparation and presentation of an annual report to the Corporate Leadership Team (CLT) and Planning Committee detailing agreements concluded; payments received; and infrastructure delivered (original implementation date: 30 June 2016).

The three findings were reopened in May 2018 and are currently reported as overdue based on their originally agreed implementation dates. Management had not addressed these historic findings at the time of our review, as it was agreed with Internal Audit that they would wait for the IA outcomes to determine how best to address both the historic and any new findings raised.

Our current review established that the backlog of historic developer agreements and value of associated contributions has not been fully analysed and quantified to determine where contributions (plus indexation and interest adjustments) should be returned to developers as per Local Government (Scotland) Act 1973 requirements.

Consequently, the original findings that were reopened will be replaced by a new High rated finding (refer 3.1 below), reflecting that the original Medium rated findings were not addressed; that the Council has been exposed to the risks noted below for a further three years; and that the volume and value of legacy contributions is likely to have increased.

The new finding will continue to be reported as overdue based on the agreed implementation date of the original finding (31 January 2016).

A further two High rated findings have been raised following completion of our current review, reflecting the need to enhance controls to ensure that the end to end developer contribution process is clearly defined and documented, with training provided across all services and teams involved; and improve the ongoing financial management of contributions received.

Our detailed findings and recommendations are included at Section 3 below.

Management response

There has been considerable progress since the 2015 Internal Audit findings were raised, but it is accepted that a further phase of work is required.

The position at March 2014, as described at page 7 of the report, was that developer contributions held in investment accounts totalled £7.378m. The 31 March 2019 position has significantly improved, as funds held in investment accounts at March 2019 that were held in these same investment accounts as at March 2014 totalled £2.653m. Based on the date of investment, accepting that this may not be the same as the day the monies were received, £1.154m of the £2.653 March 2019 position was invested in 2013/14.

The report states that of the £7.378m mentioned above, as at 31 March 2014, transport infrastructure contributions aged in excess of five years totalled £5.090m. Of the monies held on investment as at 31 March 2019, the amount which was held on investment prior to 31 March 2009, which is directly comparable to the £5.090m, is now £0.790m, of which £0.491m relates to transport. There is potential for some of these schemes to have been completed, however, and the remaining contributions will be reviewed in the second phase of our work plan as detailed in our management response to finding 1, recommendations 1.1 and 1.2 below.

These actions will be embedded within a robust end to end process to address the points raised in finding 2 below, along with other work to address the IA recommendations.

3. Detailed findings

1. Backlog of legacy developer contributions — High

Position as at October 2015

A Medium rated finding was raised in the audit of Planning Controls and the Local Development Plan completed in October 2015 reflecting the need to review legacy developer contributions.

The report highlighted that as at March 2014, developer contributions held in investment accounts totalled £7,377,870. Of this balance, funds aged in excess of 5 years relating to transport infrastructure developments totalled £5,090,108.

Finance confirmed that £3,499,850 of the £5M had been identified as 'other infrastructure' developments that was ring-fenced for specific ongoing projects, and were engaging with Transport Planning to establish the position in relation to the balance of £1,590,258. An additional balance of £706,410 that had not been transferred to investment accounts, was also being investigated, leaving a total historic balance of £2,296,668 to be reviewed and addressed.

Outcome of the Council wide self attestation exercise completed in February 2018

As part of the self-attestation exercise performed across the Council in February 2018, management confirmed that the actions agreed to address legacy contributions had been not been implemented, and the finding was reopened in May 2018.

Outcomes of current review completed August 2018

Review of the current process established to manage developer contributions confirmed that there remains a backlog of legacy developer contributions where:

- timeframes specified in legal agreements have expired;
- the conditions of the legal agreement have not been met.
- the specified purpose is no longer relevant; and
- the Council has delivered linked infrastructure from the Capital Investment Programme and would be entitled to drawdown corresponding contributions.

This backlog has not been fully analysed to determine where contributions (plus indexation and interest adjustments) should be returned to developers, and the volume of agreements and value of associated contributions has not yet been quantified.

Consequently, the original finding that was reopened will be replaced by this new High rated, reflecting that the original Medium rated finding was not addressed; that the Council has been exposed to the risks noted below for a further three years; and that the volume and value of legacy contributions is likely to have increased.

The new finding will continue to be reported as overdue based on the agreed implementation date of the original finding (31 January 2016).

Risks

- potentially significant adverse reputational consequences for the Council.

1.1 Recommendation – review of developer contributions held in the Finance database

A full review of all developer contributions held in the Finance database should be performed and all entries reconciled to amounts held on deposit and/or the general ledger. All contributions held on deposit, but marked as “expired” or “due to expire” should be considered as part of the risk-based review detailed at recommendation 2 below;

Agreed management action - review of developer contributions held in the Finance database

A full review of all developer contributions held in the Finance database will be performed, and all entries reconciled to amounts held on deposit and/or in the general ledger.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Hugh Dunn, Head of Finance; Alison Henry, Corporate Finance Senior Manager; Rebecca Andrew, Principal Accountant; Michael Thain, Head of Place Development; David Leslie, Chief Planning Officer; John Inman, Service Manager;

Agreed Implementation Date: 30 September 2020

1.2 Recommendation – retrospective review of historic developer contribution legal agreements

1. a risk based review of historic developer contribution legal agreements should be performed to determine whether:
   - the terms of the agreement have been fulfilled and the associated developer funds used on relevant infrastructure developments;
   - the terms of the agreement have or have not been fulfilled, and no developer contributions were received; and
   - the terms of the agreement have not been fulfilled and the Council is currently holding funds that should be returned to the developer.
2. where agreements have not been fulfilled, and no contributions were received, the developers should be contacted to confirm that the agreement is void and no longer applicable;
3. where agreements have not been fulfilled and funds are held by the Council, the developer should be contacted to arrange reimbursement of funds (including interest); and
4. a check should be performed prior to reimbursement to confirm that the value to be refunded has been accurately calculated.

Agreed Management Action – retrospective review of historic developer contribution legal agreements

Planning has worked with Finance to identify the status of legacy contributions identified in 2015. Planning accepts that the status of the remaining £2.3 million backlog needs to be identified, and any associated actions identified and recorded.

Whilst an agreed implementation date of 30 September 2020 is noted below, priority will be given to completing these actions as quickly as possible.

1. the audit recommendations detailed above will be implemented. Finance and planning will work together to determine the risk based sample to be included in the review.
   - for the sample selected, Planning will determine whether or not the terms of the agreement have been fulfilled
   - where agreements have been fulfilled, Finance will determine whether developer contributions have been received and applied.
   - where agreements have not been fulfilled and the Council is holding developer funds, the management action specified at 2.3 below will be applied.

2. an internal record will be maintained of agreements that have not been fulfilled to prevent services from drawing down contributions to support any development work. Developers will not be advised that agreements are void and no longer applicable, as (under legislation) only developers can seek to discharge the agreement; and
3. and 4 where agreements have not been fulfilled and funds are held by the Council, the developer will be contacted (where they can be traced) to ascertain whether they would accept reimbursement of funds. Where this is the case, a value should be agreed between the Council and the developer that reflects interest and indexation (where applicable) and reimbursed.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Michael Thain, Head of Place Development; David Leslie, Chief Planning Officer; John Inman, Service Manager; Hugh Dunn, Head of Finance; Alison Henry, Corporate Finance Senior Manager; Rebecca Andrew, Principal Accountant; Nick Smith, Head of Legal and Risk; Kevin McKee, Senior Legal Manager; Graham Nelson, Senior Solicitor.

Agreed Implementation Date: 30 September 2020

2. End to end developer contribution processes, procedures, and training — High

Review of the end to end process applied to determine the infrastructure requirements associated with planning applications; the associated costs; contributions required from developers; and ensure that funds are received within agreed timeframes established that:

- the end to end process has not been documented. Consequently, inconsistent processes based on individual preferences are applied by planning officers covering the East and West of the city;
- no detailed guidance is available to support planning offers with the assessment of infrastructure requirements (via consultation and review of the Action Programme (AP)) associated with proposed planning developments, and determination of costs;
- only one case officer is assigned to each planning application, and the current position in relation to the progress with the planning application and developer contributions is not consistently recorded on the Uniform system;
- there is no standard pro forma or guidance detailing the nature and granularity of the details required from other services to support preparation of the developer contribution proposal and finalisation of the legal agreement;
- developer contribution proposals for submission to the Development Management Sub-Committee (DMSC), and legal agreements are inconsistent in terms of structure and content;
- no ongoing quality assurance is performed by planning managers throughout the process. Whilst developer contribution proposals are reviewed prior to submission to the DMSC, a standard review process is not applied;
- estimated costs and associated contributions are not shared with developers prior to sending them the draft legal agreement;
- for developments where low value contributions are required, a legal agreement is not always established. IA was informed that a cheque is received from the developers and banked;
- the majority of developer contribution legal agreements are outsourced to external legal firms for preparation, with the associated costs incurred by the developers. No check is performed by the internal legal team to ensure that sufficient information has been provided to support preparation of the draft agreement, and there is also a significant difference between the internal and

external legal rates applied to calculate the recharge to developers, to ensure that they are not financially disadvantaged;

- Finance is not notified when contributions are finally agreed with developers. Instead, they are notified by Planning (although not always consistently) when the first contribution instalment is received;
- key person dependencies have been identified in Finance and Planning in relation to recording and monitoring contributions received;
- induction and ongoing training has not been developed and implemented for all planning officers and service areas involved in determining; agreeing; and managing developer contributions; and
- There is no established process to communicate with the Action Programme (AP) Board to ensure that they are made aware of all developer contributions received; funding gaps between expected and actual developer contributions enabling the AP financial model to be updated; and details of additional infrastructure requirements identified by planning case officers or consultees.

Risks

- lack of knowledge and understanding of the end to end developer contribution process;
- delays in finalising and agreeing developer contributions, resulting in delays in planning approval;
- Key person dependencies;
- insufficient information to support developer contribution proposals for submission to the Development Management Sub-Committee (DMSC) that could potentially result in inappropriate decisions;
- insufficient information provided to external legal firms to support preparation of legal agreements resulting in significant volumes of queries; delays; and increased costs;
- significant changes to draft legal agreements due to lack of ongoing developer consultation resulting in delays and increased costs;
- developer contributions received are not identified and appropriately allocated;
- unutilised contributions are not reallocated (where permitted) or returned to developers;
- infrastructure requirements included in the Action Programme (AP) supporting the Local Development Plan (LDP) and the supporting costing model are not updated to reflect any changes arising from individual planning applications; and
- potential breach of historic developer contribution legal agreements.

2.1 Recommendation – process documentation, guidance, and standardised documentation

1 the end to end process applied to determine the infrastructure requirements associated with planning applications; the associated costs; contributions required from developers (including interest and indexation to be applied to contributions received); finalise and agree legal agreements; ensure that funds are received within agreed timeframes; management of contributions received: and spending/delivery of infrastructure will be clearly documented and agreed by all service areas involved in the process;

2 the process will be immediately updated to reflect any significant legislative changes, and re communicated. Otherwise the process will be reviewed and refreshed annually;

3 an internal threshold should be established detailing the value and complexity threshold for infrastructure developments above which a legal agreement is required, and the contribution threshold for the Management Sub-Committee (DMSC) considering applications should be reviewed in parallel.

4 detailed guidance will be developed and implemented for planning officers detailing the end to end process and timeframes required from a planning perspective. These will include (but should not be restricted to) the need to document whether a legal agreement is required; the requirement to engage with developers throughout the process; confirmation of how funds will be received and identified (for example invoices issued with funds received via cheque payment or direct credit); and the need to ensure that the AP Board and Finance are made aware of all agreed developer contributions; and

5 standard documents will be designed and implemented to ensure that all information required is obtained from service areas; that consistent assessments are used in planning reports; consistently formatted reports are provided to Committee; and that all necessary information is provided to external solicitors.

Agreed Management Action – process documentation, guidance, and standardised documentation

Planning is working with Finance and Legal Service on a number of key areas of the end to end process. Significant progress has been made including; the pilot and use of a transport officer proforma, to identify and detail infrastructure requirements: and the introduction of standard legal agreements. Planning continues to work with legal services to finalise developer contribution templates for planning officers and this will inform a standardised approach to key consultee infrastructure requests.

All Internal Audit recommendations will be implemented as detailed above (with the exception of 3), with Planning leading the process.

As an alternative to IA recommendation 3, the rationale detailing why either no agreement; or a section 69 or 75 agreement has been developed and applied, will be documented.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Michael Thain, Head of Place Development; David Leslie, Chief Planning Officer; John Inman, Service Manager; Hugh Dunn, Head of Finance; Alison Henry, Corporate Finance Senior Manager; Rebecca Andrew, Principal Accountant; Nick Smith, Head of Legal and Risk; Kevin McKee, Senior Legal Manager; Graham Nelson, Senior Solicitor.

Agreed Implementation Date: 31 March 2020

2.2 Recommendation – quality assurance

1 Planning will develop and implement a developer contribution quality assurance process, designed to ensure that the end to end process has been consistently applied and that there is sufficient detail recorded prior to consideration of applications through the delegated or Development Management Sub-Committee (DMSC) process and prior to legal services instruction;

2 quality assurance checks will also ensure that planning officers have accurately recorded the current position in relation to both planning application and developer contribution on Uniform or any other appropriate system;

3 A standard checklist will be designed and used to record the outcomes of quality assurance reviews; and

4 All quality assurance findings must be addressed prior to submission of proposals to the DMSC and legal.

Agreed Management Action – quality assurance

Planning has made significant progress on specific parts of the contributions process, and will deliver other improvements to this process to address the recommendations. The capture and tracking of the financial contributions will be performed using the Council's PPSL accounts receivable system.

The Planning team's existing quality assurance process will be extended to include the end to end developer contributions process to be designed and applied as per recommendation 1.

The quality assurance process will cover the areas recommended by Internal Audit at 1 to 4 above, including use of the Council's PPSL accounts receivable system to record and monitor financial contributions received

ISO accreditors will also be requested to include the Developer contributions quality assurance process within the scope of their review which is scheduled for completion by October 2020.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Michael Thain, Head of Place Development; David Leslie, Chief Planning Officer; John Inman, Service Manager; Hugh Dunn, Head of Finance; Alison Henry, Corporate Finance Senior Manager; Rebecca Andrew, Principal Accountant; Nick Smith, Head of Legal and Risk; Kevin McKee, Senior Legal Manager; Graham Nelson, Senior Solicitor.

Agreed Implementation Date: 31 December 2020

2.3 Recommendation – legal agreements and rates

1. Legal should design and implement a review of all information provided by planning prior to submission to external legal firms to ensure that it is complete, and can be easily understood to minimise the volume of subsequent queries and associated costs; and
2. Legal should revisit their internal charging structure in relation to developer contributions to ensure that these are aligned with the rates charged by external legal firms.

Agreed Management Action – legal agreements and rates

Legal Services has developed a contributions template for use by planning officers prior to the determination of an application where contributions are required. Planning will continue to work with Legal Services to refine and finalise the template.

1. Legal Services will develop a template which will contain a drop down list of all information required to be filled in by Planning officers for every developer agreement, prior to a minded to grant status being issued by Planning.
2. To ensure consistency, Legal Services will apply a revised hourly charge rate based on a blended rate of the charges made by existing external firms preparing developer contribution legal agreements. This rate will be reviewed annually to ensure consistency with rates being charged under any new framework

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nick Smith, Head of Legal and Risk; Kevin McKee, Senior Legal Manager; Graham Nelson, Senior Solicitor.

Agreed Implementation Date:

30 June 2019 for implementation of template application of revised hourly charge; and

30 June 2020 for completion of first annual review of hourly charges

2.4 Recommendation – Induction and refresher training

1 Induction and ongoing refresher training covering all aspects of the developer contribution process should be designed and implemented (at least annually) for all new and existing employees; and

2 Training content should be reviewed on a regular basis (at least annually) to ensure that any legislative and process changes are reflected.

Agreed Management Action – induction and refresher training

Planning has a continuous programme of officer training which has included legal agreements, developer contributions and the Action Programme. Planning have scheduled refresher training on contributions and invited officers from other services**.**

1 All Internal Audit recommendations related to induction and refresher training will be implemented as detailed above. The training will include those employees from Planning; Finance and Legal Services who are involved in the developer contributions process; and

2 Training content will be reviewed at least annually, and will be updated (when required) to reflect any legislative and process changes.

Owner: Paul Lawrence, Executive Director of Place

Contributors: Michael Thain, Head of Place Development; David Leslie, Chief Planning Officer; John Inman, Service Manager; Hugh Dunn, Head of Finance; Alison Henry, Corporate Finance Senior Manager; Rebecca Andrew, Principal Accountant; Nick Smith, Head of Legal and Risk; Kevin McKee, Senior Legal Manager; Graham Nelson, Senior Solicitor.

Agreed Implementation Date: 30 September 2019

3. Ongoing management of developer contributions — High

Our review of the ongoing management of developer contributions received established that:

- whilst Planning advises Finance of expected contributions, accurate matching of funds received to the relevant development is not always possible as payments received do not include references to the supporting planning applications;
- Finance does not have sufficient information to allocate developer contributions against the specific general ledger cost centres associated with each development. Instead, funds are allocated to a general cost centre within the Service Area;
- where only part of a contribution can be accurately matched to a specific development, the balance is posted to an ‘unallocated money’ account. Finance circulate details of the funds included in this account weekly to relevant teams across the Council to identify owners and allocate the funds;
- developer contributions are not included as a standing agenda item in meetings held between Finance and other service areas
- the only record of the value of individual developer contributions is a spreadsheet (the contribution spreadsheet) maintained by one Finance team member;
- the contribution spreadsheet is not reconciled to the value of developer contributions recorded in the relevant general ledger accounts, or funds used for investment by Treasury. The contributions spreadsheet is also not shared with the service areas; and
- no evidence is currently required to support drawdown of s75 funds by either services or Treasury.

Risk

- funds received are not identified as developer contributions; are not allocated to the correct general ledger codes related to the specific development; and / or remain in the 'unallocated money account' for a significant period;
- inability to accurately trace and identify developer contributions in the event of a request from a developer to modify or discharge the agreement;
- the developer contribution spreadsheet (the only record of contributions received) may be incomplete and / or inaccurate; and
- inappropriate / unauthorised use of developer contributions that is not aligned with the purpose specified in legal agreements.

3.1 Recommendation – identification and allocation of developer contributions

1 Finance will be provided with details of all finalised developer contribution legal agreements; planning application references; and relevant general ledger codes to enable identification and accurate allocation of developer contributions received;

2 developers will be asked to quote either the legal agreement or planning application reference on all contribution payments;

3 Finance will engage with planning to obtain guidance re treatment of funds received in instances where the expected contributions detailed in the legal agreement do not match the actual value received;

Agreed Management Action – identification and allocation of developer contributions

Planning has commenced use of the PPSL accounts receivable system. The use of the system by planning officers ensures clear invoicing for individual contributions, streamlined payments and robust cross departmental referencing and addresses the recommendations above. This system is shared with Finance and ensures contribution payments are easily tracked back to specific infrastructure requirements.

Management accepts the control weaknesses identified considers that the following actions represent a more robust response:

1. planning will issue invoices for all developer contributions falling due using the PPSL accounts receivable system (or its successor), ensuring income is coded to the correct general ledger codes;
2. developers will be asked to quote the invoice numbers on all contribution payments.
3. recommendation 3 is accepted - Finance will engage with planning to obtain guidance re treatment of funds received in instances where the expected contributions detailed in the legal agreement do not match the actual value received

Owner: Paul Lawrence, Executive Director of Place

Contributors: Michael Thain, Head of Place Development; David Leslie, Chief Planning Officer; John Inman, Service Manager; Hugh Dunn, Head of Finance; Alison Henry, Corporate Finance Senior Manager; Rebecca Andrew, Principal Accountant; Nick Smith, Head of Legal and Risk; Kevin McKee, Senior Legal Manager; Graham Nelson, Senior Solicitor.

Agreed Implementation Date: 31 March 2020

3.2 Recommendation – ongoing maintenance of developer contributions

1 the contribution spreadsheet maintained by Finance will continue to be maintained as the main record of developer contributions received;

2 the spreadsheet will be regularly updated to reflect developer contributions received; allocation of funds to service areas; and transfer to, and receipt of funds from, Treasury;

3 allocation of interest and indexation applied (where relevant) to developer contributions will also be recorded on the spreadsheet;

4 the content of the spreadsheet will be regularly reconciled to the relevant general ledger cost centres where developer contribution funds have been allocated, to confirm completeness and accuracy;

5 reconciliations performed will be subject to ongoing management review to confirm that the position has been accurately reconciled, and all exceptions addressed;

6 the spreadsheet will be shared with Planning on an ongoing basis (at least monthly) and will be discussed at meetings held between Finance and Planning to confirm completeness and accuracy of content and address any unresolved issues;

7 appropriate controls will be developed and applied to the spreadsheet (for example, password protection and cell protection) to ensure that the content cannot be inadvertently amended;

8 previous versions of the spreadsheet will be maintained to ensure that any historic queries raised in relation to developer contributions can be addressed;

9 guidance on management of developer contributions will be developed and applied to reduce the potential risk of key person dependency; and

10 Finance will request evidence to support drawdown of developer contributions from service areas. Copies of the evidence provided will be retained with the contribution spreadsheet to provide a clear audit trail of utilisation of developer contributions.

Agreed Management Action – ongoing maintenance of developer contributions

All recommended actions will be implemented as set out above.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Hugh Dunn, Head of Finance; Alison Henry, Corporate Finance Senior Manager; Rebecca Andrew, Principal Accountant

Agreed Implementation Date: 30 September 2020

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on 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 or brand 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 or brand 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 or brand of the organisation.
Low	A finding that could have a: • ***Minor*** impact on the organisation's 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.

Appendix 9

The City of Edinburgh Council

Internal Audit

Communities and Families Self-Assurance Review

Communities and Families

Draft Report

1 May 2019

Project number CF1802

·EDINBVRGH·
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk, and Best Value Committee in March 2018. 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

In 2013 the Executive Director of Communities and Families (C&F) had concerns over the lack of information available to inform their view on school related issues that required comment in their annual assurance statement with the exception of health and safety as school health and safety related issues were identified through the ongoing Corporate Health and Safety audit programme and review of health and safety performance metrics. The annual assurance statements include assurances from Directors on the effectiveness of controls operating across their services and support the Chief Executive's Council wide annual assurance statement that is included in the annual accounts.

Consequently, a school's assurance framework was launched as a pilot in 2015 to assess effectiveness of operational; health and safety; and information governance controls across schools and centres within Communities and Families.

This involved Internal Audit; Corporate Health and Safety; and Information Governance visiting 30 schools and centres between 2015 and 2017 to assess the design and effectiveness of their operational processes and controls. Two reports were issued (February 2015 and January 2017), highlighting good practice in each of the areas looked at by the combined Internal Audit/Corporate Health and Safety team and identified areas where improvements were required.

Following completion of the pilot, Internal Audit reduced its involvement in the Assurance Framework in 2017/18 and ceased the programme of visits to establishments. They recommended that Communities and Families set up a programme of peer reviews to replace the Internal Audit component of the programme. The C&F Principal Risk Manager worked closely with the second line business partners, including the Council's Health and Safety Manager, and latterly, Internal Audit, to develop and implement the current Self Assurance Framework (the framework) designed to support completion of the C&F Annual Governance Statement by providing an informed view on the effectiveness of controls across first line C&F establishments responsible for delivering services.

In 2018 the Principal Risk Manager and C&F Operations Manager undertook a series of visits to 15 establishments to support the work of the framework; a report on the findings was provided to the Education Children and Families Committee on 14 August 2018 and can be viewed at Self Assurance Report.

The framework is essentially an annual self-attestation provided by all establishments, confirming the effectiveness of their operating controls, and is performed by completing a 'Survey Monkey' questionnaire, for which comprehensive guidance is provided and updated annually. Communities and Families received an ALARM (Association of Local Authority Risk Managers) award in June 2018 for the design and implementation of the framework.

It is understood that the framework is unique across the Council with Communities and Families the first to implement a self-assurance approach to support completion of the Director's annual governance statement that has identified some control weaknesses (for example, Essential Learning and the introduction of ParentPay).

Ongoing effectiveness of health and safety controls continue to be assessed by Corporate Health and Safety as part of their rolling Corporate H&S Audit Programme, and ongoing review of health and safety performance metrics in addition to responses received in relation to health and safety through the self assurance framework.

Scope

The scope of this review assessed the design adequacy and operating effectiveness of the key controls supporting operation of the Self Assurance Framework.

Whilst no specific self-assurance framework risk is currently included in the Communities and Families risk register, the framework, and this review, covers a number of operational service delivery risks.

Sample testing involved visiting 8 establishments in October to review and discuss the framework returns completed covering the period 1 April to 31 March 2018.

Our audit work concluded on 7th November 2018, following discussion with the Operations Manager and Principal Risk Manager regarding the results of our testing, and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Summary of findings raised	
High	1. Framework design and effectiveness

Opinion

Communities and Families should be commended for proactively initiating this unique approach to obtaining assurance (to support the Director's annual assurance statement) and remediating any control gaps identified in relation to compliance with applicable Council policies, and the effectiveness of operational controls across 153 of their establishments.

Recognition of the need for the framework and its implementation demonstrates a high level of risk awareness by Communities and Families senior management, and the concept is also aligned with the three lines of defence model and good practice applied in other industries (for example, financial services apply similar frameworks across their retail branch operations).

It is also acknowledged that the framework continues to be refined to reflect regulatory and Council policy changes; and new and emerging risks, with ongoing support provided by Risk Management.

However, our review confirmed that significant enhancements are required to improve the design of the framework; encourage higher questionnaire response rates; and confirm the accuracy of responses received, to ensure that it completely and accurately supports the Director's annual assurance statement.

Given the weaknesses identified with the design and effectiveness of the framework, it has not been possible to determine whether Communities and Families establishments are consistently complying with key Council policies; confirm that key operational controls are being consistently and effectively applied; and ensure that any control weaknesses identified are effectively resolved.

Consequently, 1 High rated finding has been raised.

The High rated finding also reflects the need to secure support for the framework from all relevant second line business areas and partners, as this is necessary to ensure that the questionnaire remains aligned with applicable legislation and Council policies; and confirm the accuracy of responses received.

Communities and Families management has advised that whilst some second line teams have been supportive, more assistance is required.

Whilst a number of weaknesses have been identified, it should also be noted that several establishments highlighted the value of the framework, as completion of the annual questionnaire requires them to be more focused on operational risk and controls; regularly assess the effectiveness of their control environment; and implement new, or enhance existing controls in response to new and emerging risks.

There is potential for significant assurance value to be delivered by the framework or a similar model, however, to achieve this, the control weaknesses identified require to be addressed. This may be constrained by the availability of resources within Communities and Families, and the availability of second line Business Partners to provide the ongoing support required.

The diagram in appendix 2 shows the expected stages involved in a self-assurance framework including the linkages to the Director's Annual Assurance Statement and the role of second line business partners and teams across the Council.

3. Detailed findings

1. Framework Design and effectiveness — High

To ensure that the framework effectively supports the Director of Communities and Families annual assurance statement, it is essential that it is adequately designed to identify any significant operational control weaknesses, and that responses received are complete and accurate.

Review of the framework design and effectiveness established that:

- completion of the questionnaire is not mandatory, although it is issued by the Director, and followed up with several completion reminder e mails. Circa 76% of the total population of Communities and Families establishments completed the 2017/18 questionnaire;
- the framework questionnaire is not fully aligned with content of the Director's annual assurance statement;
- in some instances, several controls are covered by one question (e.g. 3 generic questions under the financial controls section cover 13 areas of compliance from the guidance) and it is unclear whether one control gap / instance of non-compliance with applicable Council policies should result in an overall negative response; although management have advised that a partially compliant option has been added to the survey;
- a total of 4 operational control gaps in relation to financial management and human resources were identified, that are not currently included in the framework questionnaire (further detail is included at Appendix 3);
- survey responses are analysed to identify thematic control gaps and instances of non-compliance for inclusion in the annual assurance statement, whilst this is a self-attestation exercise, no independent validation is performed, which would be beneficial to confirm the accuracy of survey responses;
- support available from second line Business Partners (who own and manage policies and frameworks) who are required to contribute to the design of the questionnaire and validate the responses; and first line Business Partners (for example Property and Facilities Management) who provide services across the establishments) is limited. Several establishments also advised that the support available from Facilities Management was not sufficient to enable them to complete some of the questions.
- limited feedback and support is provided to establishments that identify control gaps and non-compliance through the survey, and support is required from Business Partners to provide advice on issues identified. There is currently no established process to ensure that the required improvements are implemented and sustained;
- Internal Audit and Corporate Health and Safety identified a total of 18 control gaps that were included in the questionnaire or supporting guidance, but had not been identified by establishments when completing the returns. Further detail is included at Appendix 3;
- management has advised that resource constraints have impacted the ability to validate questionnaire responses; provide support to resolve weaknesses in the internal control environment; and could impact ongoing operation of the framework.

Risk

The following risks describe what Audit believe may be the worst case scenario if control gaps are not addressed via implementation of recommendations:

- The Director's Assurance Statement may potentially be incomplete and inaccurate if the self-assurance returns are not completed correctly;
- Establishments may not be aware of applicable Council policies, procedures; and key controls that should be applied to manage the risks associated with their operations; and
- Significant control gaps and non-compliance with applicable Council policies may not be identified and resolved.

1.1 Recommendation –Ongoing Feasibility of the Framework

1 As the ongoing feasibility of the framework is significantly dependent upon support from second line business partners, Communities and Families senior management should engage with second line senior management to secure their ongoing collective support for the design and refresh of the questionnaire, and validation of survey responses;

2 If second line support is secured, agreed management actions and implementation dates will be provided in relation to recommendations 1.2 to 1.7 included in this report, with ongoing implementation progress monitored by Internal Audit; and

3 If second line support cannot be secured, then management should design and implement an alternative approach to obtain the level of assurance required to support the annual governance statement.

Agreed Management Action

1. Without additional support from all key second line Business areas and Business Partners, it is difficult for C&F to ensure the relevant questions are included in the questionnaire each year. Support is also required to validate the responses and ensure the survey accurately reflects the internal control environment.

   Communities and Families will engage with key Business Partners to identify if the required support can be provided to address Internal Audit's recommendations.
2. Agreed.
3. Alternatively, if the support is not available from Business Partners, C&F will fall back in line with the majority of other directorates that do not currently operate self assurance frameworks.

Owner: Alistair Gaw, Executive Director of Communities and Families **Contributors:** Nickey Boyle, Senior Executive Administrator; Michelle McMillan, Principal Risk Manager	**Agreed Implementation Date:** 31 July 2019

1.2 Recommendation – Reinforce the requirement for all establishments to complete the questionnaire

1. Management should consider whether the requirement to complete the survey returns should be mandatory;
2. If mandatory completion is agreed, the requirement should be communicated across all establishments;
3. If mandatory completion is not agreed, management should reinforce the importance of completion of the questionnaire, and follow-up with establishments that do not provide returns to understand the reasons for non-completion.

Agreed Management Action

N/A – management responses will only be provided once the future assurance approach has been decided.

Owner: **Contributors:**	**Agreed Implementation Date**
1.3 Recommendation - Questionnaire design	
1. The self-assurance questionnaire should be aligned to the Director's annual assurance Statement to ensure that establishments are aware of all applicable Council policies; procedures; and key controls, and confirm whether they are consistently and effectively applied; 2. The questionnaire should be mapped (at least annually) to all key Council policies and operational processes to ensure that it completely and accurately reflects any significant changes (for example, the new sickness absence policy; drivers' policy; and GDPR requirements); and 3. Where possible, survey questions should be aligned with one key control / Council policy to ensure that holistic and unclear responses are not received; or use of 'partially compliant' survey responses supported by explanations should be introduced.	
Agreed Management Action	
N/A – management responses will only be provided once the future assurance approach has been decided	
Owner: **Contributors:**	**Agreed Implementation Date**
1.4 Recommendation – Independent validation of returns	
1. A process should be implemented to validate completeness and accuracy of returns on a sample basis prior to their consolidation and inclusion in the annual assurance statement; and 2. Any potentially significant errors identified in the return should be followed up on a risk basis with the relevant establishment to confirm the accurate position.	
Agreed Management Action	
N/A – management responses will only be provided once the future assurance approach has been decided	
Owner: **Contributors:**	**Agreed Implementation Date**
1.5 Recommendation - Feedback and support	
Where significant and thematic control gaps and instances of policy non-compliance are identified, support and guidance should be provided to establishments to ensure that appropriate remedial actions are implemented and sustained.	
Agreed Management Action	
N/A – management responses will only be provided once the future assurance approach has been decided	
Owner: **Contributors:**	**Agreed Implementation Date**
1.6 Recommendation - Framework review meetings	

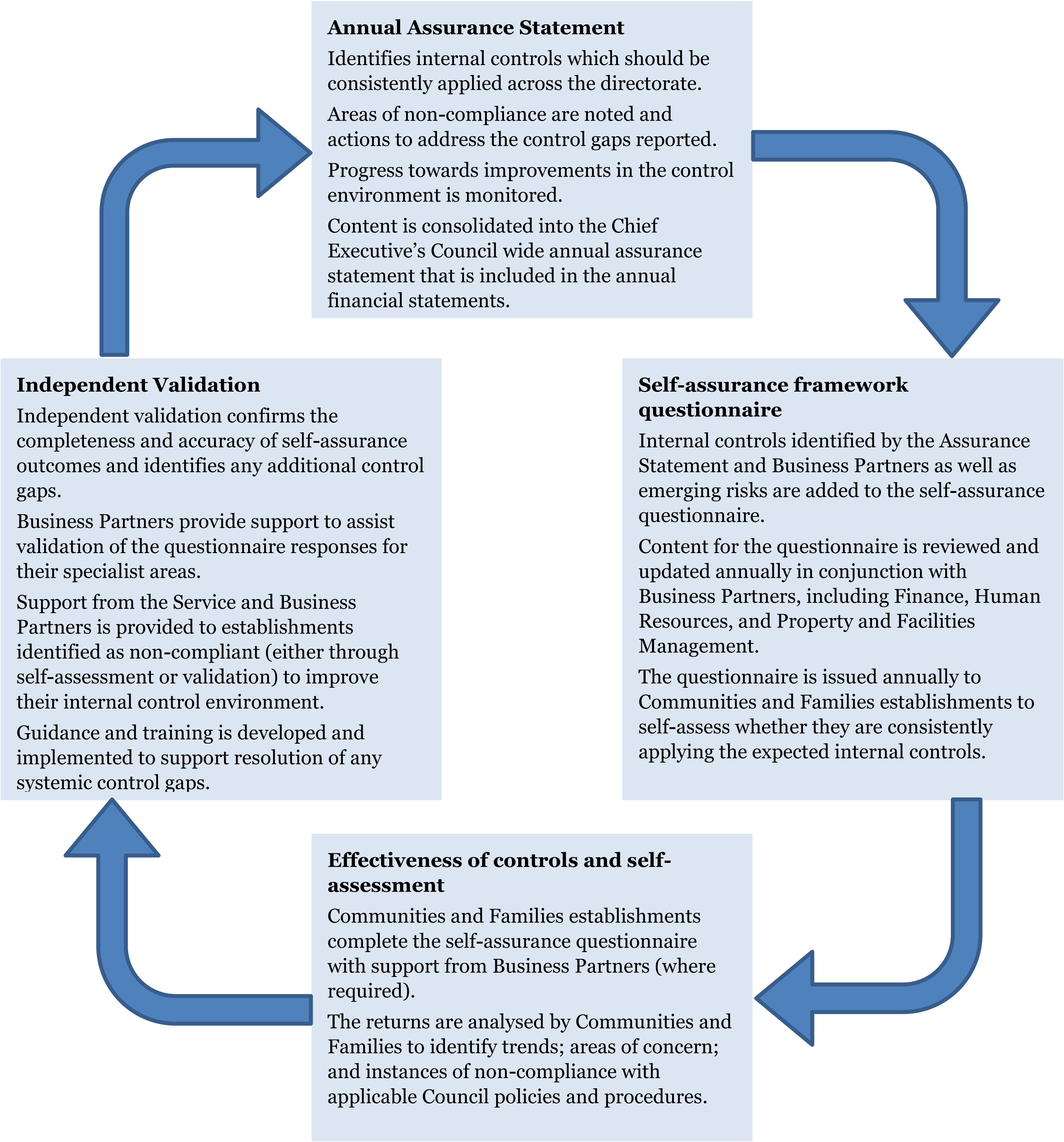
Communities and Families senior management should chair and attend the six-monthly review meetings designed to review and refresh the framework, to ensure that their experience, and details of any new and emerging risks and issues are discussed and incorporated (where appropriate).	
Agreed Management Action	
N/A – management responses will only be provided once the future assurance approach has been decided	
Owner: **Contributors:**	**Agreed Implementation Date**
1.7 Recommendation - Capacity	
Management should review existing resource capacity and ensure that sufficient resources are allocated to support ongoing operation of the framework.	
Agreed Management Action	
N/A – management responses will only be provided once the future assurance approach has been decided	
Owner: **Contributors:**	**Agreed Implementation Date**

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on 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 or brand 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 or brand 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 or brand of the organisation.
Low	A finding that could have a: • ***Minor*** impact on the organisation's 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.

Appendix 2 - Self-assurance framework design

The following flow diagram highlights the expected stages in a standard self-assurance framework that is aligned with the three lines of defence model. While several of these stages are included in the C&F self-assurance model, a number of improvements are required as detailed in the High rated finding raised.



Annual Assurance Statement

Identifies internal controls which should be consistently applied across the directorate.

Areas of non-compliance are noted and actions to address the control gaps reported.

Progress towards improvements in the control environment is monitored.

Content is consolidated into the Chief Executive's Council wide annual assurance statement that is included in the annual financial statements.

Self-assurance framework questionnaire

Internal controls identified by the Assurance Statement and Business Partners as well as emerging risks are added to the self-assurance questionnaire.

Content for the questionnaire is reviewed and updated annually in conjunction with Business Partners, including Finance, Human Resources, and Property and Facilities Management.

The questionnaire is issued annually to Communities and Families establishments to self-assess whether they are consistently applying the expected internal controls.

Effectiveness of controls and self-assessment

Communities and Families establishments complete the self-assurance questionnaire with support from Business Partners (where required).

The returns are analysed by Communities and Families to identify trends; areas of concern; and instances of non-compliance with applicable Council policies and procedures.

Independent Validation

Independent validation confirms the completeness and accuracy of self-assurance outcomes and identifies any additional control gaps.

Business Partners provide support to assist validation of the questionnaire responses for their specialist areas.

Support from the Service and Business Partners is provided to establishments identified as non-compliant (either through self-assessment or validation) to improve their internal control environment.

Guidance and training is developed and implemented to support resolution of any systemic control gaps.

Appendix 3 - Issues identified from establishment visits

	Issue	Number of establishments where issue was identified	Issue identified in self-assessment (for establishments in the IA sample)	Included in framework questionnaire/guidance?	Issue included in Directors Assurance Statement?
Ref	**Significant issues identified by Internal Audit during visits**				
1.	**Financial management** - there is not a school fund constitution and committee with minuted meetings, and/or the school fund is not audited.”	7	No	No	No
2.	**Financial management** - lack of segregation of duties regarding banking of income.	5	No	Yes - guidance	No
3.	**Financial management** - out of date bank signatories remain on accounts.	7	No	No	No
4.	**Human resources -** Limited recording of right to work interviews and stages in MyPeople (iTrent).	5	Identified by one school	Yes - questionnaire	No
5.	**GDPR and records management** - Pupil files stored in an unlocked cabinet / cupboard that is supposed to be locked - however was unlocked when visited and the room was also unlocked.	2	No	Yes - questionnaire	No
6.	**Financial management** - significant variance between Pebble (fund management system) cash at hand and the cash on site. Lack of understanding if a separate imprest account is still required.	4	Identified by one school	Yes - guidance	No
7.	**Financial management** - no evidence retained following cash counts/ reconciliations.	5	Identified by one school	Yes - guidance	No

	Issue	Number of establishments where issue was identified	Issue identified in self-assessment (for establishments in the IA sample)	Included in framework questionnaire/guidance?	Issue included in Directors Assurance Statement?
8.	**Financial management** - no access to Pebble (fund management system).	1	No	N/A	No
9.	**Financial management** - large amount of cash on site potentially outwith insurance limits.	2	Identified by one school	Yes - guidance	No
10.	**Financial management** - both nurseries/EYC do not complete the quarterly budget monitoring statement.	2	Identified by one nursery	Yes - questionnaire	No
11.	**Equalities** - No log of bullying and prejudice incidents (no request from the department for a nil return)	1	No	Yes - questionnaire	No
12.	**Equalities** - Staff have not received equalities and diversity training within 3 years	1	Yes	Yes - questionnaire	No
13.	**Equalities** - The Head Teacher has not undertaken training in Managing Allegations of Abuse Against Staff and Volunteers by completing the e-learning module annually.	1	Yes	Yes - questionnaire	No
14.	**Financial management** - lack of awareness/ completion of the financial controls eLearning.	7	Identified by one school	No	No
15.	**Corporate Governance** - Register of interest/hospitality registers – no request to submit the register to the department (including nil returns)	8	No	No	No

	Issue	Number of establishments where issue was identified	Issue identified in self-assessment (for establishments in the IA sample)	Included in framework questionnaire/guidance?	Issue included in Directors Assurance Statement?
16.	**GDPR and records management** - no procedures for reporting information governance incidents, data breaches and non-compliance.	1	Yes	Yes	Yes
17.	**Resilience** - Red button folder available, however there was limited evidence this had been communicated with staff.	1	No	Yes	No
	Framework issues identified by establishments during visits				
18.	Issues regarding communication with FM/ centre manager uncomfortable signing off the FM sections.	4	N/A	Yes - guidance	Yes
19.	Limited support for areas marked as non-compliant (Some schools noted receiving a standard email).	6	N/A	N/A	No
20.	Would like more feedback on comments and evidence that these are acted upon.	5	N/A	N/A	No
21.	The guidance provided regarding information governance is lacking clarity.	2	N/A	N/A	Yes
	Thematic issues identified by Corporate Health and Safety (during ongoing audits) that were not identified by establishments (note that only thematic issues are included and a larger number of individual Health and Safety Issues have been identified)				
22.	Insufficient recording of Statutory Inspections	3	Identified by one school	Yes - guidance	Yes
23.	Window restrictors suitability check has been carried out in last 12 months.	4	Identified by one school and one	Yes - questionnaire	Yes

	Issue	Number of establishments where issue was identified	Issue identified in self-assessment (for establishments in the IA sample)	Included in framework questionnaire/guidance?	Issue included in Directors Assurance Statement?
			school did not submit a response		
24.	Regular walk round inspections carried out by SSO covering internal and external fabric of the building and services.	3	No	Yes - questionnaire	No
25.	Adequate H&S risk assessments in place for all curricular activities, as applicable.	2	No	Yes - guidance	No