Culture and Communities Committee

10.00am, Tuesday 11 September 2018

Internal Audit Update Report: 1 January – 31 July 2018 – referral from the Governance, Risk and Best Value Committee

Item number	9.5
Report number	
Wards	All

Executive summary

The Governance, Risk and Best Value Committee on 31 July 2018 considered a report which detailed the Internal Audit progress for the period 1 January to 31 July 2018

The report has been referred to the Culture and Communities Committee on the recommendation that high and medium risk findings from audit reports be submitted to their parent Committee for information.

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Terms of Referral

Internal Audit Update Report: 1 January – 31 July 2018

Terms of referral

1.1 On 31 July 2018, the Governance, Risk and Best Value Committee considered a summary of the findings and status of work from the Internal Audit plan of work. Additional reviews were to be added to the plan where considered necessary to address any emerging risks and issues identified during the year, subject to formal approval by the relevant committee.

1.2 The report by the Chief Internal Auditor indicated that Internal Audit recruitment had been successful and the team now expected to be at full complement by the beginning of October 2018.

1.3 Work had commenced on the 2018/19 annual plan, however, delivery had been impacted by the ongoing resourcing challenges. It had been agreed with PwC that resources would be provided in August to support delivery of three 2018/19 reviews.

1.4 The Governance, Risk and Best Value Committee agreed:

1.4.1 To note the risks associated with the 21 High rated findings raised in the 17 Council reports.

1.4.2 To note that the 2 Lothian Pension Fund reports had been presented to the Pensions Committee for scrutiny

1.4.3 To refer the 6 reports noted in Appendix 1 as potentially being of interest to the Audit and Risk Committee of the Edinburgh Integration Joint Board (EIJB), to that Committee.

1.4.4 To note that no reports were referred by the EIJB Audit and Risk Committee to the Governance Risk and Best Value Committee at their meetings in February, March and May 2018.

1.4.5 To note the current position with resources and successful recruitment.

1.4.6 To note the progress with the 2018/19 annual plan and recent IA priorities.

1.4.7 To ask for an update to the next meeting on the ability of the 18/19 Plan to deliver its outcomes.

1.4.8 To refer the audit report on CCTV noted in Appendix 1 to the CCTV Working Group for consideration.

1.4.9 To refer the high and medium risk findings to each executive committee as appropriate.

1.4.10 To ask for a further report on the processes involved for making changes to the 2017/18 Internal Audit Plan.

For Decision/Action

2.1 The Culture and Communities Committee is asked to note the attached audit reports with high and medium risk findings concerning CCTV Infrastructure.

Background reading / external references

Webcast of Governance, Risk and Best Value Committee – 31 July 2018

Laurence Rockey
Head of Strategy and Insight

Contact: Louise Williamson, Assistant Committee Officer

Email: louise.p.williamson@edinburgh.gov.uk | Tel: 0131 529 4264

Links

Appendices	Appendix 1 – Internal Audit Update Report: 1 January 2017 – 31 July 2018 – report by the Executive Director of Resources

Appendix 1

Governance, Risk and Best Value Committee

10.00am, Tuesday 31 July 2018

Internal Audit Update Report: 1 January – 31 July 2018

Item number	7.2
Report number	
Executive/routine	
Wards	
Council Commitments	

Executive Summary

This report provides details of Internal Audit (IA) reviews completed in the period; recent changes to the 2017/18 IA plan; and updates on resourcing; commencement of the 2018/19 Internal Audit plan; and IA priorities.

Internal Audit has now issued a total of 33 2017/18 audit reports to the City of Edinburgh Council (the Council) the Lothian Pension Fund (LPF) and the Edinburgh Integration Joint Board (EIJB), with 19 issued between 1 January and 31 July 2018. This included 15 reports for the Council; 2 for LPF; and 2 for the EIJB.

Of the 19 reports issued to the Council, two have been presented separately to the Committee for scrutiny. The remaining 17 reports include 65 findings (21 High; 34 Medium; and 10 Low).

A total of 6 reports are recommended for referral from the GRBV to the EIJB Audit and Risk Committee. No reports have been referred by the EIJB Audit and Risk Committee during the period.

IA recruitment has been successful and the team is now expected to be at full complement by the beginning of October 2018.

Work has commenced on the 2018/19 annual plan, however, delivery has been impacted by ongoing resourcing challenges. It has been agreed with PwC that resources will be provided in August to support delivery of three 2018/19 reviews.

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Report

Internal Audit Update Report: 1 January – 31 July 2018

1. Recommendations

1.1 Committee is recommended to:

1.1.1 Note the risks associated with the 21 High rated findings raised in the 17 Council reports and consider if further clarification or immediate follow-up is required with responsible officers for specific items;

1.1.2 Note that the 2 LPF reports have been presented to the Pensions Committee for scrutiny;

1.1.3 Refer the 6 reports noted in Appendix 1 as potentially being of interest to the EIJB Audit and Risk Committee;

1.1.4 Note that no reports were referred by the EIJB Audit and Risk Committee to GRBV at their meetings in February; March and May 2018.

1.1.5 Note the current position with resources and successful recruitment; and

1.1.6 Note progress with the 2018/19 annual plan and recent IA priorities.

2. Background

2.1 Internal Audit is required to deliver an annual plan of work, which is scoped using a risk-based assessment of Council 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 relevant Committees.

2.2 IA progress and a summary of findings raised in the reports issued are presented to the Governance, Risk, and Best Value Committee quarterly.

2.3 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.

2.4 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.

2.5 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.

3. Main report

Audit Findings for the period

3.1 A total of 33 2017/18 audit reports have now been issued to the to the Council (27); LPF (4); and the EIJB, with 23 issued between 1 January and 15 July 2018.

3.2 This included 19 reports for the Council; 2 for LPF; and 2 for the EIJB.

3.3 Of the 19 reports issued to the Council, the Building Standards, and Edinburgh Building Services (Housing Property Services) reports have been presented separately to the Committee for scrutiny.

3.4 The remaining 17 Council reports included a total of 65 findings (21 High; 33 Medium; and 10 Low). The majority of the findings raised (40%) were included in the Care Homes Assurance (4 High; 12 Medium; 4 Low) and Drivers Health and Safety (3 High and 6 Medium) audits. Details of completed reports are included at Appendix 1, with individual reports provided in Appendix 2 (following the order in Appendix 1).

3.5 The 2 LPF reports have been presented to the Pensions Audit Committee for scrutiny. These reports included a total of 11 findings (4 High; 3 Medium; and 4 Low).

3.6 The 2 EIJB reports were presented to the July EIJB Audit and Risk Committee, and it was agreed that these should be referred to the GRBV.

A total of 6 Council reports are recommended for referral from the GRBV to the EIJB Audit and Risk Committee (refer Appendix 1).

Changes to the 2017/18 IA Plan

3.7 The Health and Social Care Partnership Care Inspectorate Follow-up review that was included in the 2017/18 audit plan has been replaced with a review of the Edinburgh Mela Ltd at the request of management, given the significant reputational risks associated with the Council's decision to provide funding to support the Mela festival. Given resource constraints it was not possible in the timescales available to undertake both reviews.

3.8 It is expected that the Mela Ltd review will be completed in early July. This review has no impact on the Council's 2017/18 Internal Audit annual opinion.

Resourcing

3.9 Recruitment has been successful with offers now accepted for all vacant roles

3.10 It is expected that the IA team will be at full complement by the beginning of October, with new team members joining on a phased basis (aligned with notice periods) from July onwards.

Progress with 2018/19 Annual Plan

3.11 Work on the 2018/19 annual plan has commenced with one audit currently in progress.

3.12 Progress with the 2018/19 plan has been impacted by ongoing resourcing challenges, and the priorities noted below.

3.13 It has been agreed with PwC that resources will be provided in August to support delivery of three 2018/19 audits.

Internal Audit Priorities

3.14 Focus for the last quarter has been directed at finalising the audit reports for the 2017/18 annual plan; recruitment; and launching the new automated follow-up process.

3.15 The new system will be launched Council wide in early July, with training delivered during the weeks of 25 June and 2 July focusing on the role and importance of IA; rebranding IA as 'your safety net'; sharing examples of best practice when finalising audit reports and providing updates and evidence to support closure of findings; and introducing the new system.

4. Measures of success

4.1 Once implemented, the recommendations contained within these reports will strengthen the Council's control framework.

5. Financial impact

5.1 No direct financial impact.

6. Risk, policy, compliance and governance impact

6.1 Internal Audit 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 Internal Audit reports.

7. Equalities impact

7.1 Not applicable.

8. Sustainability impact

8.1 Not applicable.

9. Consultation and engagement

9.1 Not applicable.

10. Background reading/external references

10.1 Building Standards Audit Report to GRBV 8 May 2018

10.2 Housing Property Audit Report to GRBV 5 June 2018

Lesley Newdall

Chief Internal Auditor

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

11. Appendices

Appendix 1 Summary of IA reports issued and findings raised during the period and recommendations for referral to the EIJB Audit and Risk Committee.

Appendix 2 Audit reports issued in period 1 January 2018 to 31 July 2018

Appendix 1 – Summary of IA reports issued and findings raised during the period and recommendations for referral to the EIJB Audit and Risk Committee.

		Findings Raised				
	Audit Review	**High**	**Medium**	**Low**	**Totals**	**Refer to EIJB**
	Council Wide					
1.	Drivers Health and Safety	3	6	0	9	Y
2.	Phishing Resilience	2	1	0	3	Y
	Safer and Stronger Communities					
3.	CCTV Infrastructure	2	0	0	2	N
	Resources					
4.	CGI Contract management	0	2	0	2	N
	Communities and Families					
5.	Foster Care Review	1	2	1	4	N
	Strategy and Insight					
6.	Resilience Assurance	2	2	1	5	Y
7.	Project Benefits Realisation	2	0	0	2	Y
	Health and Social Care – note that both reviews include management actions owned by Resources (Customer)					
8.	Care Homes	4	12	4	20	Y
9.	Social Work Centre Bank Account Reconciliations	2	0	0	2	Y
10.	Review of Social Care Commissioning	1	1	0	2	*
11.	Health and Social Care Purchasing Budget Management	4	0	0	4	*
	Place					
12.	Port Facility Security Plan	1	4	1	6	N
13.	H&S Waste and Recycling	0	4	2	6	N
	Lothian Pension Fund					
14.	Payroll Outsourcing	1	0	1	2	N
15.	Pensions Tax	1	1	0	2	N
	Totals	**26**	**35**	**10**	**71**	

* Reports referred to the Governance, Risk and Best Value Committee from the Edinburgh Integration Joint Boards Audit and Risk Committee

Appendix 2 – Audit reports issued in period 1 January 2018 to 31 July 2018

The City of Edinburgh Council

Internal Audit

CCTV Infrastructure

Final Report

2 April 2018

SSC1703

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2017/18 internal audit plan approved by the Governance, Risk, and Best Value Committee in March 2017. 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) operates a close circuit television (CCTV) camera estate across public spaces; housing blocks; schools; bus lanes and Council buildings. The total operational cost of public space is £955,354 with income of £128K generated.

Provision of CCTV services is non-statutory, with the service provided to support public security and the prevention and detection of crime in line with the following Council priorities and pledges:

- 'Safe and empowered communities' (CP4) with the objective of ensuring that 'People and communities are safe and protected'.
- Single Outcome Agreement, (SO4) 'Edinburgh's communities are safer and have improved physical and social fabric'.
- Coalition pledges (P32) 'Develop and strengthen local community links with the police'.

Police Scotland are the main users of CCTV footage to support criminal prosecutions, and use the Council's CCTV services (under the terms of a partnership agreement developed by a sub group of the Police and Fire Scrutiny Committee in 2017) with the objective of reducing crime and antisocial behaviour in communities.

During 2016/17 the Police requested 1,369 CCTV image reviews with 152 resulting in court evidence packages being prepared. Seven portable camera assessments were also performed.

Retention, archiving and destruction of CCTV footage, and sharing footage with third parties is governed by the requirements of the Data Protection Act (1998). These processes will also require to be compliant with the new General Data Protection Requirements due to be implemented in May 2018. There is also a general requirement to work within the parameters of the Human Rights Act, Regulation of Investigatory Powers Act (RIPSA) and finally the Council's Code of Conduct.

Specifically, providers of CCTV services in public spaces require to comply with the requirements of the Scottish Government's National Strategy for Public Space CCTV in Scotland (March 2011),

Boston Networks was recently commissioned to review the condition of the Council's current CCTV estate and its operational status, with the outcomes published in August 2017.

Their report recommended implementation of a CCTV strategy to focus on the location and scope of control centres, and confirmed that significant investment is required to upgrade the technology infrastructure of the estate, recommending investment in an internet protocol (IP) based CCTV estate to replace the current analogue system.

Scope

As the Boston Networks review concluded on the requirement to develop a strategy and upgrade the existing CCTV estate, the scope of our review focused on the controls in place to manage the following CLT top risks:

- Information governance
- Maintaining service with less resource

Testing was undertaken on a sample basis across the period 1st April 2017 to 31st August 2017 across the Public Space, Security, and Concierge service areas.

2. Executive Summary

Total number of findings

Critical	-
High	2
Medium	-
Low	-
Advisory	-
Total	**2**

Summary of findings

Our review established significant strategic and operational control gaps in relation to delivery of CCTV services across the Council. Consequently, two 'High' rated Findings have been raised.

Our first Finding reflects the impact of a lack of corporate CCTV strategy (the service is currently run at a loss across three Service Areas); failure to progress the requirement for significant investment in the CCTV technology infrastructure identified from the Boston Networks review; and lack of a clearly documented corporate plan to ensure that all CCTV operations are compliant with current Data Protection Act requirements, and will be compliant with General Data Protection Regulations effective from 25th May 2018

Our second Finding reflects a number of significant control gaps in Service Area operational processes that have resulted in instances of non-compliance with Data Protection Act requirements, the Council's Information Security Policy and Records Management policies.

Our detailed findings and recommendations are included at Section 3: Detailed Findings. Further details of the testing outcomes for each of the Service Areas reviewed as at 30th September 2018 (Public Space, Security, and Concierge) are included at Appendix 1

3. Detailed Findings

1. CCTV Strategy

Finding
There is currently no consolidated corporate strategy and standard operational procedures supporting consistent and legislatively compliant delivery of CCTV Services across Service Areas, and no established recharge process to enable recovery of CCTV costs incurred by the Council. There has also been no progress in addressing the failings highlighted in the Boston Network report which highlighted that significant investment in the CCTV technology infrastructure was required to support future delivery of the service. Finally, there is no clearly documented corporate plan to ensure that all CCTV operations will be compliant with General Data Protection Regulations effective from 25th May 2018.

Business Implication	Finding Rating
• Failure to operate consistently and effectively, and risk of potential legislative breaches. • Reputational risk associated with major failure in CCTV infrastructure resulting in inability to provide the Service • Potential financial loss associated with failure to recharge costs. • Potential non-compliance with new GDPR regulations.	**High**

Action plans	
Recommendation	**Responsible Officer**
1. A corporate CCTV Strategy and standard operational procedures should be designed and implemented. This should include establishment of a centralised CCTV delivery budget and a recharge process to enable recovery of costs and support income maximisation (where possible). 2. Standard processes should be developed for implementation across all service areas providing CCTV services. These should be aligned with applicable legal and regulatory requirements and should include (as a minimum) procedures covering: • Approval and requisition of new CCTV equipment, • Prioritisation of requests for cameras in new locations and their allocation across geographical sites, • Identification and repair of damaged equipment, • Retention, archiving and destruction of footage that are aligned with the Council's Records Management policy and Data Protection Act requirements, and • Approval of requests for footage and the process for sharing footage in a secure manner.	Senior Manager, Community Justice

3. An action plan should be designed and implemented to address the CCTV infrastructure failings highlighted in the Boston Network report, and a request submitted to Finance and the relevant Council Committees for funding to support investment. 4. A corporate CCTV risk register recording the consolidated risks associated with delivery of CCTV services should be prepared. These should include details of action plans to mitigate the risks identified, and appropriate action owners. The risk register should also be subject to regular ongoing review to ensure that risk and action plans remain appropriate. 5. A consolidated asset register should be prepared and maintained to record all CCTV equipment owned by the Council, its condition and location. 6. A corporate business continuity plan should be designed and implemented to support recovery of the CCTV services across all locations in the event of a disaster. 7. A gap analysis should be performed and a corporate plan developed to ensure the service will be compliant with GDPR by 25th May 2018.	
Agreed Management Action	**Estimated Implementation Date**
1. A CCTV working group has been established that is chaired by an Elected Member. The Lead Officer is the Manager, Community Safety. Three sub working groups have also been established. The sub 'Strategy' group has been tasked with developing an overall CCTV Strategy with the objective of 'future proofing' the CCTV service. The strategy will include recommendations for establishment of a centralised CCTV delivery budget and a recharge process to enable recovery of costs and support income maximisation (where possible). It is not yet possible to commit to an agreed implementation date for the strategy which is likely to be longer term. It has therefore been agreed with Internal Audit that the finding will be closed and development and approval of the strategy, with further IA reviews scheduled to consider effective implementation of the strategy.	27th September 2019
2. The sub 'Policy and Procedures' group will deliver a standard set of CCTV operational processes and procedures to be implemented across all three CCTV service areas. These will include the areas noted in the audit recommendation.	28th September 2018
3. The objective of the sub 'Tactical Working Group' is to oversee and implement the upgrade of public space CCTV in line with Council wide technology and ensure it is compatible for future integration of council service. This will include the identification of funding sources to support the necessary CCTV investment.	27th September 2019
4. 5 & 6 It is expected that the strategy document will recommend the establishment of one centralised CCTV operations centre and data centre for the Council. This will be supported by appropriate risk registers; asset registers and resilience plans. The requirement for standardised approaches in these areas will be reflected in the strategy document produced. Meantime, Security are undertaking exercise to	27th September 2019

fully document all security systems (including CCTV) in detailed Asset Registers 7. Information Governance has performed their GDPR readiness review of three CCTV areas, and the questionnaire has been completed. Action plans are currently being developed.	29th June 2018

2. CCTV Operations

Finding
Lack of corporate strategy and standard operational procedures has resulted in three Service Areas (Public Space, Security, and Concierge) managing their CCTV services independently with differing standards of operational processes and controls, with examples of non-compliance with applicable legislation evident in all three areas. The following control gaps were identified consistently across all three Service Areas, and have been discussed separately with each: 1. Data protection regulations (the Seventh Principle), and the CEC Information Security Policy (ISO/IEC 2700) were non-compliant in Security Services area as the CCTV file server and downloaded CCTV images were stored in an open, regularly unstaffed room that was occasionally open to public access. 2. There is no evidence of regular internal or peer reviews of CCTV operations as required by the National Strategy for Public Space CCTV to ensure compliance with Data Protection Act requirements. 3. Service Area procedures supporting CCTV operations were not up to date and had not been subject to periodic review. and Current records management processes applied within the three service areas are not fully compliant with current Data Protection Act requirements and the Council's Records Management policy. An example of this was that all three service areas had a different document retention process, with Security applying a process of retaining footage until they have been informed that a Police case file is closed; Public Safety retaining footage until told by the court that the footage can be destroyed; and Concierge retaining footage for a year before deletion. 4. Risks associated with the operation of CCTV services have not been identified and recorded on Service Area risk registers. 5. No induction training and ongoing training and development is provided for CCTV team members to ensure they are aware of all applicable legislation; legislative changes and operational processes for the Service Area.

Business Implication	Finding Rating
• Financial penalty and reputational damage associated with breach of Data Protection legislation and Council Records Management policies. • Failure to operate consistently and effectively, and risk of potential legislative and National Strategy breaches. • Employees may unknowingly breach applicable legislation or Council policies.	High

Action plans	
Recommendation	**Responsible Officer**

1. Immediate action should be taken to secure access to the Security Services file server and downloaded CCTV images and a request made to the Information Governance team to carry out a review of any new procedure, ensuring compliance with relevant policies and legislation. 2. Internal and peer reviews should be incorporated in operating procedures and performed as per the requirements of the National Strategy for Public Space CCTV to ensure Data Protection Act compliance 3. Service Area procedures should be reviewed and aligned with Corporate CCTV and Records Management procedures (with specific focus on retention periods for CCTV images on systems, and retention of downloaded CCTV footage), and reviewed at least annually. 4. Risks associated with delivery of CCTV services should be identified and recorded on the relevant Service Area risk registers. 5. Induction and ongoing training should be delivered to all CCTV staff and appropriate records maintained of completion.	1. Security Manager, Property and Facilities Management 2. to 5 - Senior Manager, Community Justice
Agreed Management Action	**Estimated Implementation Date**
1. The server hardware at NPH has been updated and is now secured behind constructed partition with air conditioning. Access is restricted by controlled entry, and the installation of air conditioning should now negate the need to leave the door open in summer to support ventilation. NPH is a 24/7 facility and would not normally be unstaffed. Security of downloaded images has been addressed with a lockable filing cabinet. All procedures have been reviewed with policy guidance updated. These will be included in the ongoing work of the Procedures Sub group of the CCTV Working Group From a DR perspective currently, all NPH alarms can be manually transferred to Waverley Court in the event of a catastrophic failure / loss of service. An upgrade CCTV viewing capability at Waverley Court (WC) is currently being scoped. The existing WC server will also be afforded better protection to future proof and prolong service life. This will include an upgrade to the capacity and capability of the default processes providing limited CCTV monitoring capability at Waverley Court. 2. Public Space supervisors undertake review of staff work on a monthly basis in line with legislation around CCTV Governance. This is to be rolled out across Security and Concierge services. Additionally, the new policies and procedures being developed will include the requirement to record that the reviews have been performed, and document the actions taken to address any gaps identified, and any Data Protection breaches. 3. The 'Policy and Procedures' sub group is developing a standard set of CCTV policy and procedures to be applied consistently across the entire council CCTV Estate. These procedures will include records management requirements for CCTV images held on systems and also downloaded CCTV images. The requirement for an annual review to confirm to incorporate any necessary changes will also be included.	27th April 2018 28th September 2018 28th September 2018

4. The Council's Risk Management team will be engaged to support a review of CCTV risk registers across all three areas, and ensure that the risk registers are refreshed. Risk registers will be standardised where possible. All security related CCTV risks have now been recorded on Property and Facilities Management risk register.	28th September 2018
5. The roll out of the new policies and procedures to be applied across all CCTV operations will be supported by employee briefings and training. The new policies and procedures will also include the requirement for induction training for all new employees and ongoing refresher training (to be delivered by each respective Service Area lead). Properties and Facilities Management has prepared a training matrix. A training provider has been also identified and training course dates established throughout 2018 for service users. A security information page is also being prepared for publishing on the Orb.	30th November 2018

Appendix 1 – Service Area Testing Outcomes as at 30th September 2018

Objective	Risks	Consolidated RAG Status	Public Space RAG status	Security RAG status	Concierge RAG status
CCTV services are subject to annual review to confirm that ongoing service provision and associated costs and benefits remains aligned with the Council's strategic objectives	Service may become misaligned with strategic objectives.	There is no consolidated strategy for provision of CCTV services across the Council, and the outcomes of the Boston Networks consultancy review have not been progressed.	No annual review performed of provision of CCTV Services by Public Space.	No annual review performed of provision of CCTV Services by Security.	No annual review performed of provision of CCTV Services by Concierge.
Processes and procedures are regularly reviewed and updated to reflect legislative changes.	Process and procedures are out of date leading to breaches in legislation and regulation.	There are no established Council wide procedures supporting delivery of CCTV services.	There are no regular reviews of existing processes and procedures to ensure that they remain aligned with applicable legal requirements.	There are no regular reviews of existing processes and procedures to ensure that they remain aligned with applicable legal requirements.	There are no regular reviews of existing processes and procedures to ensure that they remain aligned with applicable legal requirements.
Supporting rationale is provided for all requests for installation of cameras.	Expenditure on CCTV assets is unnecessary and inappropriate.	There is no established Council wide process for prioritising requests for purchase of CCTV equipment	Additional equipment cannot be ordered as the current assets are now obsolete. Lack of action on Boston report is a big risk for this area	There is no established process for prioritising the purchase of CCTV equipment.	No information has been provided, therefore assessed as a control gap and rated red.
A clear prioritisation process has been established to support allocation of the estate across public spaces.	CCTV service does not support the needs of CEC or other users	No clear process has been established across the Council for prioritisation of allocation of equipment across geographic locations.	There is a lack of evidence that the Regulation of Investigatory Powers Act (RIPSA) requirements are followed for Police requesting provision and use of the Mobile camera units. There was a lack of evidence showing how the rest of the camera use was prioritised. Community Improvement Partnerships discuss crime and antisocial	Current Security Services CCTV equipment is functional, but in need of significant investment in to fully network the system and enhance monitoring capability at NPH. to support ongoing service provision. requests cannot be met. There are increasing concerns that current	The Calder project was ringfenced Housing Property Capital provision. It is being used only for the upgrade and improvement of CCTV provision with the three Calder, but does not cover remaining concierge services. Any additional requests cannot be met. .

Appendix 1 – Service Area Testing Outcomes as at 30th September 2018

Objective	Risks	Consolidated RAG Status	Public Space RAG status	Security RAG status	Concierge RAG status
			behaviour statics and allocate redeployable cameras were there is a need, request form and process in place	contractual arrangements with SPIE will not fully deliver the maintenance of existing systems.	
A process has been established to identify all damaged CCTV cameras and ensure that they are repaired in a timely manner	CCTV infrastructure becomes unfit for purpose.	There is no established Council wide process to support identification and repair of CCVTV equipment.	SPIE are contracted to maintain the infrastructure as and when required. There is a structured process in place for requesting maintenance but when a camera is damaged beyond repair the only way to maintain this is to decommission a lesser used working camera and utilise its parts.	Camera faults are reported daily through a formal process and these faults are either repaired by the Security Officer with the technical skills to do so or it is reported to Property and Facilities Management who then in turn contact SPIE to maintain. There are significant delays between the date reported and the date this is passed to Property and Facilities Management for action.	All cameras are reviewed as part of the night shift duty check. Any faults are reported and the cameras that have broken down are being replaced with new digital technology.
CCTV footage is generated and stored in a secure environment with access restricted to only authorised personnel.	Footage is not protected in accordance with Data Protection Legislation and CEC's Information Security Policy, and is accessible by unauthorised personnel	There is no Council wide policy or process detailing the requirements for secure storage of CCTV footage.	• An ad hoc storage process is applied. • Access restrictions are documented and communicated. • There is independent review of activity in place but this is not documented or formalised.	• The server for the Security CCTV area is in an open office and when the weather is warm the main security door is wedged open enabling access by any member of the public walking in off the street. • This is where the footage downloaded for Court packages is also kept in drawer cabinets which are not locked.	• Footage is generated onsite in the concierge office. • Any images removed are stored in a locked cupboard. • The disk the images are recorded on remains in place and is recorded over every 30 days.

Appendix 1 – Service Area Testing Outcomes as at 30th September 2018

Objective	Risks	Consolidated RAG Status	Public Space RAG status	Security RAG status	Concierge RAG status
A process has been established to ensure that all requests from third parties for access to / copies of CCTV footage are formally approved.	Images and Data are shared inappropriately with no audit trail of transactions.	There is no Council wide process supporting approval of third party requests for access to copies of CCTV footage.	• There is a very robust process in place for the receipt and response to third party requests for access to footage. • This process has not been assessed against recent legislation but formal approval for the request is obtained and retained.	There is a process in place for requesting footage but there is no evidence that this has been signed by the Police to confirm evidence of receipt.	• There is a written procedure included within the request forms showing the official process in place for Concierge staff and Police to follow. • Requests are made in writing but there is no formal approval from the officer requesting the footage or for the Concierge making the copy. • The process is not governed by a policy or aligned regularly with legislation. • There is no SLA established with the Police to ensure consistent application of the process for requesting access to footage.
Processes and Procedures are in place providing guidance on the retention, archiving and destruction of CCTV footage	Lack of compliance with regulatory requirements (Data Protection Act) and Council Records	There is no formal Council wide procedure covering retention, archiving and destruction of CCTV footage in line with applicable regulatory requirements and Council policies.	• There is a good procedure in place but it has not been formally documented. • There is a gap around the destruction of CCTV footage, there is confusion	• There are no documented processes and procedures in place. • All training is based on verbal update and 'on the job' experience.	• Footage downloaded and retained for evidence by the Police is subject to review and destruction. • Images captured by cameras is kept for 31

Appendix 1 – Service Area Testing Outcomes as at 30th September 2018

Objective	Risks	Consolidated RAG Status	Public Space RAG status	Security RAG status	Concierge RAG status
	Management policies.		over where this responsibility lies.		days in accordance with the legislation however there is no official guidance for this and the process applied is not consistent with the other CCTV service areas.
Footage is retained, archived, and destroyed in line with policies and procedures	Breach of CEC policies and procedures resulting in fines and penalties.	There are no established Council wide procedures to ensure that footage is retained and archived in lie with policies and procedures.	There is a good process in place for obtaining, retaining, and archiving footage, but there is no process in place for destroying footage resulting in the archive room almost reaching maximum capacity.	There are no written or communicated process in place applying the principles of CEC's Records Management Policy	There is a process in place for obtaining, retaining, and archiving footage but there are no policies and procedures to link this too and there is nothing in place to govern destruction of data.
CCTV footage can only be provided to approved parties and shared through secure channels	Breach of Data Protection act by inappropriate sharing of CCTV data	There are no established Council wide procedures to ensure that footage is only provided to approved parties and shared securely.	There are effective procedures in place to ensure footage is only provided to approved parties and is shared securely.	Footage is only provided to Police and will be shared via cd however this procedure is not documented and linked with current CEC Records Management policy	Process in place but not documented and linked to relevant legislation
An asset register has been established and regularly updated to reflect additions and disposals, record locality of all CCTV cameras and infrastructure.	Assets are lost or misappropriated without recourse through lack of asset management	There is no consolidated Council wide asset register detailing the CCTV equipment owned the Council, or the condition and location of the equipment.	There is no Public Space asset register, however SPIE are obliged to review the public Space CCTV and provide the section with a list of all equipment held. This has not been adequately completed. Complete, asset register is in place, awaiting photographic	There is no Security Services asset register,	There is a log of all cameras and equipment for the Calder Flats Concierge service

Appendix 1 – Service Area Testing Outcomes as at 30th September 2018

Objective	Risks	Consolidated RAG Status	Public Space RAG status	Security RAG status	Concierge RAG status
			evidence of condition of each camera		
Risk registers for all service areas include relevant CCTV related risks	Preventable risks may occur due to lack of risk management	There is currently no risk register supporting provision of CCTV Services across the Council, and the Boston consultancy report recommendations have not been progressed.	Appropriate CCTV risks are included in the Public Space risk register.	There are no risk registers in place for the Security Service.	There are no risk registers in place for the Concierge Service.

Appendix 2 - 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 3 – Terms of Reference

Safer Stronger

Terms of Reference – CCTV Infrastructure Management and Maintenance

To: Harry Robertson, Interim Head of Service, Safer and Stronger

From: Lesley Newdall, Chief Internal Auditor Date: 8th September 2017

Cc: Michelle Miller, Interim Chief Officer for the Health and Social Care Partnership
Bruce Strang, Chief Information Officer
Kevin Wilbraham, Record and Information Compliance Manager
Shirley McLaren, Community Justice Senior Manager
Will Boag, Security Manager
Jennifer Hunter, Tenant and Resident Services Manager
Alistair Gaw, Executive Director of Communities and Families
Stephen Moir Executive Director of Resources
Paul Lawrence Executive Director of Place

This review is being undertaken as part of the 2017/18 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2017.

Background

The City of Edinburgh Council (CEC) operates a close circuit television (CCTV) camera estate across public spaces; housing blocks; schools; bus lanes and Council buildings.

The total cost for the CCTV services provided by the Council is £833K and generates income of £128K. The police are the main users of CCTV footage to support criminal prosecutions.

Retention, archiving and destruction of CCTV footage is governed by the requirements of the Data Protection Act (1998) and will also require to be compliant with the new General Data Protection Requirements due to be implemented in May 2018. The Data Protection Act also governs sharing of CCTV footage with third parties.

Boston Networks was recently commissioned to review the CCTV estate used across the Council and its operational status, with the outcomes published in August 2017.

The report recommended implementation of a CCTV strategy to focus on the location and scope of control centres, and confirmed that significant investment is required across the estate to establish an effective and efficient service. The report also recommended moving from an historic analogue to an internet protocol (IP) based CCTV estate.

Scope

As the Boston Networks review has concluded on the requirement to develop a strategy and upgrade the existing CCTV estate, the scope of our review will focus on the controls in place to manage the following CLT top risks:

- Information governance

- Maintaining service with less resource

Testing will be undertaken on a sample basis for the period 1st April 2017 to 31st August 2017.

Limitations of Scope

The scope of our review is outlined above. Following publication of the Boston report our review will not assess the quality of the current CCTV estate infrastructure.

Approach

Our audit approach is as follows:

- Obtain an understanding of the CCTV services through discussions with key personnel, review of systems documentation and walkthrough tests;
- Identify the key risks associated with the provision of CCTV services;
- Evaluate the design of the controls in place to address the key risks; and
- Test the operating effectiveness of the key controls.

The sub-processes and related control objectives included in the review are:

Sub-process	Control Objectives
Strategic alignment	• The CCTV service is subject to annual review to confirm that ongoing service provision and associated costs and benefits remain aligned with the Council's strategic objectives. • Risk registers for all service areas include relevant CCTV related risks.
Estate allocation and maintenance	• An asset register has been established and regularly updated to reflect additions and disposals, and record the location of all CCTV cameras and infrastructure. • Supporting rationale is provided for all requests for installation of cameras. • A clear prioritisation process has been established to support allocation of the estate across public spaces. • A process has been established to identify all damaged CCTV cameras and ensure that they are repaired in a timely manner.
Use and retention of CCTV footage	• CCTV footage is generated and stored in a secure environment with access restricted to only authorised personnel. • A process has been established to ensure that all requests from third parties for access to / copies of CCTV footage are formally approved.
Data Protection Act compliance	• There are documented processes and procedures in place supporting retention, archiving and destruction of CCTV footage. • There are documented procedures in place to ensure that CCTV footage is only provided to approved parties, and is shared in a secure manner. • Processes and procedures are regularly reviewed and updated to reflect legislative changes. • Footage is retained, archived and destroyed in line with policies and procedures.

	• The location of all CCTV footage is recorded and updated to reflect issue to and receipt from third parties.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	0131 469 3216
Hugh Thomson	Principal Audit Manager	0131 469 3147
Lorraine Twyford	Internal Auditor	0131 469 3145

Key Contacts

Name	Title	Role	Contact Details
Shirley McLaren	Community Safety Senior Manager	Review Sponsor	0131 529 5035
Robert Meikle	Security Services	Key Contact	0131 529 7077
Jennifer Hunter	Concierge Services	Key Contact	0131 529 7532
Harry Robertson	Community Safety Senior Manager	Departmental contact	0131 553 8237
Michelle Miller	Safer Stronger	Head of Service	0131 553 8520

Timetable

Fieldwork Start	11/09/17
Fieldwork Completed	27/09/17
Draft report to Auditee	06/10/17
Response from Auditee	20/10/17
Final Report to Auditee	27/10/17

Follow Up Process

Where reportable audit findings are identified, the extent to which each recommendation has been implemented will be reviewed in accordance with estimated implementation dates outlined in the final report.

Evidence should be prepared and submitted to Audit in support of action taken to implement recommendations. Actions remain outstanding until suitable evidence is provided to close them down.

Monitoring of outstanding management actions is undertaken via monthly updates to the Director and their elected audit departmental contact. The audit departmental contact liaises with service areas to ensure that updates and appropriate evidence are provided when required.

Details of outstanding actions are reported to the Governance, Risk & Best Value (GRBV) Committee on a quarterly basis.

Appendix 1: Information Request

It would be helpful to have the following available prior to our audit or at the latest our first day of field work:

- Risk registers for all three areas
- Budget statements for 1 April to 30 August
- Latest Regulation of Investigatory Powers Act Scotland (RIPSA) 2000 report
- Policy documentation
- Procedures for management of CCTV data/images
- Asset register for Criminal Justice, Security and Concierge CCTV services.

This list is not intended to be exhaustive; we may require additional information during the audit which we will bring to your attention at the earliest opportunity.