

Glasgow City Council Internal Audit Section

Committee Summary

NRS – Public Space CCTV Information Management

Item 7(f)

25th January 2023

1

1 Introduction

- 1.1 As part of the agreed Internal Audit plan, we have carried out a review of Public Space Closed-circuit Television (PSCCTV) information management.
 - 1.2 Glasgow City Council has 429 fixed public space CCTV cameras across the city as well as 98 traffic cameras and 8 re-deployable cameras. Public space CCTV and traffic cameras are monitored by Neighbourhoods, Regeneration and Sustainability (NRS) staff, from the Glasgow Operations Centre (GOC) based in the Council's Eastgate building.
 - 1.3 It is important that the Council stores its PSCCTV data in a way that prevents unauthorised access, misuse or loss of data. PSCCTV images may be shared with other Council services and Police Scotland as well as occasionally other third parties including HMRC and the DWP. However, the Council must ensure it only shares its PSCCTV data in line with the requirements of the Data Protection Act 2018 (DPA) and the relevant Council procedures.
 - 1.4 The Council's public space CCTV utilises a Physical Security Incident Management system (PSIM) which has two primary applications which are Situator and NiceVision. Both are applications developed and managed by Qognify who are contractually managed by the Council's IT partner CGI.
- However, NRS have a system administrator to support day to day operations and a technical team who maintain the cameras.
- 1.5 The scope of the audit was to ensure there are sufficient and appropriate controls in place covering the Council's PSCCTV operations regarding the management of PSCCTV data. The scope of the audit included:
 - Reviewing relevant policies and procedures regarding the identification and mitigation of information security risks for public space CCTV;
 - Ensuring that roles and responsibilities have been clearly defined including where third parties request and/or access the Council's PSCCTV data;
 - Reviewing compliance with the Council's information security policies and guidance including third party access and information sharing protocols/ data sharing agreements;
 - Ensuring the Council's PSCCTV data is adequately secured to prevent unauthorised access, misuse or loss; and
 - Ensuring that, where appropriate, the Council's policies and procedures regarding PSCCTV information security are aligned to the DPA and National Strategy for Public Space CCTV in Scotland.

2 Audit Opinion

- 2.1 Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and 4 recommendations which management should address.

3 Main Findings

- 3.1 Generally the expected key controls are in place and operating effectively. NRS' PSCCTV service is certified for compliance with the English Biometrics and Surveillance Camera Commissioner's Code of Practice (no Scottish equivalent is currently in place). Logs of the PSCCTV data that have been shared were viewed on site, and for a sample of items request forms and receipts could be produced where appropriate
- 3.2 The PSCCTV Code of Practice (CoP) notes that the Council recognises that the PSCCTV system gathers information on individuals and their activities and documents how this should be processed in compliance with the relevant legislation.
- 3.3 However, we found a number of areas where controls should be strengthened. Appropriate procedures are in place to manage and escalate risks but the PSCCTV risk register does not include risks and mitigating controls in place relating to the sharing of PSCCTV data with third parties.
- 3.4 Data sharing agreements were obtained which document the roles and responsibilities between PSCCTV and Police Scotland, the DWP and HMRC, however these are not up to date and often reference the former Community Safety Glasgow (CSG) ALEO; additionally the versions of the agreements viewed were not signed by CSG/GCC. CSG no longer exists with all staff and services having been transferred into the Council in 2019.
- 3.5 An overarching data sharing agreement for Police Scotland, which will include PSCCTV, is being developed by the Council's Head of Information and Data Protection Officer but this is yet to be implemented.
- 3.6 We have been advised that those removing PSCCTV data are reminded of their responsibilities regarding the data, however this is not documented.
- 3.7 The GOC is accessed via multiple doors which are operated using ID passes. We have been advised that a list of ID passes which can access the GOC is received and reviewed on a quarterly basis. Documentation for this could not be provided however, although evidence of requests for leavers to be removed was provided.

- 3.8 The PSCCTV service does not retain authorisation for access to the PSIM platform once they are passed over to CGI. We have been advised that the leavers process includes the removal of users from the PSIM platform and that a user review is completed quarterly. Whilst evidence has been received that users are removed and that user reviews have taken place, these are not formally documented.
- 3.9 From a sample of 10 system users we identified one user who retired in September 2022, which was not picked up as part of the most recent review.
- 3.10 Although the Council's Acceptable Use Policy applies to third party users of the PSIM system (e.g. Police Scotland) they are not currently required to complete the Council's information security training or sign acceptance of the policy. We have been advised that this could be challenging due to the number of third party users who need to access the system.
- 3.11 The Information Commissioner's Office (ICO) registration number documented by PSCCTV could not be found on the ICO's public register. A review of PSCCTV related documentation including their Code of Practice found that the ICO registration number listed was out of date and had not been updated to reflect CSG's transfer into the Council.
- 3.12 An action plan is provided at section four outlining our observations, risks and recommendations. We have made 4 recommendations for improvement. The priority of each recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	0
Medium	Less critically important controls absent, not being operated as designed or could be improved.	2
Low	Lower level controls absent, not being operated as designed or could be improved.	2
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

- 3.13 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.
- 3.14 We would like to thank officers involved in this audit for their cooperation and assistance.
- 3.15 It is recommended that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the attached Action Plan.

4 Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Documentation is up to date, there are clearly defined responsibilities, and all parties are aware of their role.				
1	Data sharing agreements were obtained which document the roles and responsibilities between PSCCTV and Police Scotland, the DWP and HMRC. However, these are not up to date and often reference the former CSG ALEO. While the data sharing agreements viewed have been signed by HMRC and the DWP these were not signed by GCC/CSG. The Police Scotland agreement was viewed on site and this version was not signed by either party. An overarching data sharing agreement for Police Scotland is being developed by the Council's Head of Information and Data Protection Officer including PSCCTV, however this is yet to be implemented. A review of other PSCCTV related documentation including their Code of Practice found that the ICO registration number listed was out of date and had not been updated to reflect CSG's transfer into the Council	PSCCTV should undertake a review of their data sharing agreements with third parties to ensure that these are still appropriate and fit for purpose. These agreements and other documentation should also be updated to reflect the integration of the former ALEO CSG into the Council. PSCCTV should work with the Council's Head of Information and Data Protection Officer to implement the Council's data sharing agreement with Police Scotland once this is available.	Medium	Management Response: Accepted Agreements will be updated to reflect the changes required from the ALEO to GCC. These will then be agreed and signed off by GCC Data Protection Team, relevant managers, and the 3rd party organisation. Officer Responsible for Implementation: Operations Manager Glasgow Operations Centre Timescales for Implementation: 30 April 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
	If PSCCTV documentation, including data sharing agreements are not kept up to date or formally agreed where relevant, Council data may be shared in a manner or to a third party which is not aligned to the relevant regulations or Council procedures			

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Access to PSCCTV data is appropriately restricted.				
2	The GOC is accessed via multiple doors which are operated using ID passes. We have been advised that a list of ID passes which can access the GOC is received and reviewed on a quarterly basis. Although evidence of requests for leavers to be removed has been provided documentation of the review process could not be obtained. Additionally, we have been advised that the leavers process includes the removal of users from the PSIM platform and that a user review is completed quarterly. While evidence has been received that users are requested to be removed and that user reviews have taken place, these are not documented. From a sample of 10 system users we identified one user who retired in September 2022, prior to the most recent review. If user reviews are not documented, there is an increased risk that they are not undertaken in the correct manner. This could result in users having access that is not commensurate with their role or retaining access after they have left the organisation.	PSCCTV should ensure that reviews are formally undertaken. In doing so they should document and retain evidence of the quarterly review process for physical access to the GOC and for the PSIM platform. This should document the users reviewed and the line manager who confirmed their access, including third parties where appropriate.	Medium	Management Response: Accepted A quarterly review process for PSIM users is already in place. A six-monthly review process for GOC access will be put in place in collaboration with building management Officer Responsible for Implementation: Operations Manager Glasgow Operations Centre Timescales for Implementation: 28 February 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: An assessment of known information risks has been performed.				
3	While procedures are in place to manage and escalate risks, the PSCCTV risk register does not include risks and mitigating controls relating to the sharing of PSCCTV data with third parties. If risks are not identified with appropriate mitigating controls there is an increased likelihood that these may not be monitored and this could result in data loss, fines, or reputational damage to the Council.	PSCCTV should review their risk register to ensure that all known information risks have been included.	Low	Management Response: Accepted The PSCCTV risk register currently has a risk in place for Information Security, but this primarily refers to internal usage. The Risk Register will be updated to include a new Information Security Risk that will highlight 3rd party access and usage. Officer Responsible for Implementation: Operations Manager Glasgow Operations Centre Timescales for Implementation: 28 February 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: PSCCTV Data is adequately secured to prevent unauthorised access, misuse, or loss.				
4	We have observed that signed receipts are retained when footage is removed from the GOC. Those removing PSCCTV footage from the GOC are verbally reminded of their responsibilities regarding the data and this is not recorded. Additionally, PSCCTV staff are not required to sign a confirmation of their responsibilities, for example only taking what is required, knowing where it is to be taken and obtaining managerial approval for doing so. We have also identified that third party users of the PSIM system are not required to complete the Council's information security training or sign the acceptable use policy. We have been advised that this would likely be challenging due to the number of third party users who need to access the system for short periods of time. Where responsibilities have been verbally accepted it would be difficult for PSCCTV to confirm that these were known if the PSCCTV data released was later found to have been used inappropriately.	PSCCTV should review their current forms and receipts regarding the removal of PSCCTV data from the GOC to include the data handling responsibilities of the party receiving PSCCTV footage, and ensure that these are signed. Additionally, PSCCTV should consider documenting the information security training that third party users with access to the PSIM platform have received. This could either be as part of the Council's training or through their own organisation.	Low	Management Response: Accepted All relevant forms will be updated to highlight responsibility of the data controller and to whom the data is passed. Discussions with primary 3rd party users will take place to discuss options in regards information security management training being documented and all relevant documents reviewed to include where relevant data management responsibilities Officer Responsible for Implementation: Operations Manager Glasgow Operations Centre Timescales for Implementation: 30 April 2023