Internal Audit Report

Surveillance Cameras (2021/22)

Final

Assignment Lead: Lucy Discombe, Senior Auditor
Assignment Manager: Paul Fielding, Principal Auditor
Prepared for: East Sussex Fire & Rescue Service
Date: April 2022

Report Distribution List

Duncan Savage, Assistant Director Resources & Treasurer
Hannah Scott-Youldon, Assistant Director – OSR
Daryll Luxford, Info Sec and DP Officer
Mark McCorkell, Senior Capital Projects Manager
Louis Thompson, Engineering Services Manager
Eddie Vine, Temporary Engineering Services Manager
Richard Moon, Station Manager Ops P&P

This audit report is written for the officers named in the distribution list. If you would like to share it with anyone else, please consult the Chief Internal Auditor.

East Sussex Fire & Rescue Service - Internal Audit Key Contact Information

Chief Internal Auditor: Russell Banks, ☎ 07824362739, ✉ russell.banks@eastsussex.gov.uk
Audit Manager: Paul Fielding, ☎ , ✉ paul.fielding@eastsussex.gov.uk
Anti-Fraud Hotline: ☎ 01273 481995, ✉ confidentialreporting@eastsussex.gov.uk

1. Introduction

1.1. The Protection of Freedoms Act 2012 (PoFA) introduced the regulation of public space surveillance cameras in England and Wales. As a result, a surveillance camera code of practice (SC Code) was issued by the secretary of state through the Surveillance Camera Commissioner to ensure that the use of cameras in public places is regulated and only used in pursuit of a specified purpose. Whilst the PoFA and SC Code are not specifically targeted at fire and rescue services (rather, local authorities and the police are the focus), the code acknowledges that "many surveillance camera systems are operated by…other public authorities", which are encouraged to adopt the code voluntarily. Therefore, the SC Code was used as an example of best practice for the purposes of this audit.

1.2. The SC code seeks to balance the need for cameras in public places with individuals' right to privacy, and it sets out 12 principles for the operation of surveillance camera systems including the need to: have a defined purpose and legitimate aim; be operated transparently so people know they are being monitored; be operated with good governance; store no more images/data than strictly required; ensure images/data are stored securely; review systems regularly (at least annually); be effective in supporting law enforcement etc.

1.3. The service should also have regard to GDPR and the Data Protection Act 2018 (DPA) when using surveillance camera systems because the cameras may capture personal information that could identify individuals. Surveillance camera systems are defined under section 29 the Protection of Freedoms Act 2012 to include: closed circuit television (CCTV), automatic number plate recognition (ANPR) systems, Body Worn Cameras, Drones and any other systems for recording or viewing visual images for surveillance purposes.

1.4. The objective of this audit was to review the effectiveness of the controls in place with regards to the deployment of surveillance camera systems in public spaces (including those on vehicles) and that any personal information captured is managed in accordance with data protection legislation.

1.5. This review is part of the agreed Internal Audit Plan for 2021/22.

1.6. This report has been issued on an exception basis whereby only weaknesses in the control environment have been highlighted within the main body of the report.

2. Scope

2.1. The purpose of the audit was to provide assurance that controls are in place to meet the following objectives:

- Deployment of surveillance camera systems in public spaces is effective, proportionate and transparent.
- The use of new and existing surveillance camera systems, and the handling and storage of any resulting data or images, complies with the Surveillance Camera Commissioner's code of practice and meets the requirements of the Authority's insurers.
- Personal information captured from surveillance camera systems are managed in accordance to the requirements of GDPR and the Data Protection Act.

3. Audit Opinion

3.1. **Partial Assurance is provided in respect of Surveillance Cameras (2021/22)**. This opinion means that there are weaknesses in the system of control and/or the level of non-compliance is such as to put the achievement of the system or service objectives at risk. *Appendix A provides a summary of the opinions and what they mean and sets out management responsibilities.*

4. Basis of Opinion

4.1. In general, governance arrangements surrounding surveillance cameras were found to be weak. There is no nominated single point of contact in relation to surveillance cameras, with responsibility being divided across service areas such as Engineering and Estates. Additionally, these roles and responsibilities are not formalised, as no policies or procedures are currently in place around surveillance cameras.

4.2. This lack of policies and procedures also means that there is no documentation covering important information such as retention periods of images and third-party access to images, to help ensure these are approached consistently and in line with the SC Code.

4.3. Statements of the need for the surveillance camera systems were found to be poor. In some instances, no such documentation (such as a Data Privacy Impact Assessment) setting out the objective of the system and legal bases for its deployment was found. In other cases, documentation was outdated or incomplete.

4.4. It was also noted that on vehicles with cameras, and at the Preston Circus building, no signage was present to advise individuals that CCTV is in place. Without this, individuals may not be aware they are being monitored, and cannot consent to this due to lack of transparency. Additionally, whilst a privacy policy is available to the public on the East Sussex Fire & Rescue Service (ESFRS) website, this makes only brief reference to surveillance camera images, without in-depth information as to how these are used.

4.5. Over the course of this audit positive steps have been taken towards implementing records of camera systems and individual cameras, with the development of records for both those on buildings and those on vehicles. This will allow for easier facilitation of reviews of cameras and compliance with the Surveillance Camera Code of Practice Going forward, the Estates team will also develop diagrams to show the location of all cameras. ESFRS' progress in this area has been taken into account when issuing this audit opinion.

4.6. Further examples of good practice were also present. Images are of a sufficient quality (including a time and date stamp), to be used as evidence where required. Additionally, no inappropriate access to surveillance camera images was found, with those from buildings accessed only by ESFRS's contracted security company and those from vehicles shared with the police when requested via a suitable Subject Access Request (SAR) form. However, it is noted that this arrangement (whereby ESFRS do not have direct access to vehicle camera footage) contributes to ESFRS not being able to claim a discount on insurance.

5. Action Summary

5.1. The table below summarises the actions that have been agreed together with the risk:

Risk	Definition	No	Ref
High	This is a major control weakness requiring attention.	2	1, 2
Medium	Existing procedures have a negative impact on internal control or the efficient use of resources.	2	3, 4
Low	This represents good practice, implementation is not fundamental to internal control.	2	5, 6
	Total number of agreed actions	**6**	

5.2. Full details of the audit findings and agreed actions are contained in the detailed findings section below.

6. Acknowledgement

6.1. We would like to thank all staff that provided assistance during the course of this audit.

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
1	**Policies and Procedures** Principle 5 of the Surveillance Camera Code states: *Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them* It is understood that although a policy and manual around surveillance camera usage in buildings was due to be implemented, this has yet to be drafted. There is also no policy or procedure in place relating to cameras on vehicles, although again, there is an aim to create and implement one. ESFRS therefore does not currently have formal policies and procedures in place relating to the usage of surveillance cameras, which would serve to support the lawful operation of surveillance camera systems, as well as ensuring consistency across the authority. Such documentation could include information on staff roles and responsibilities, retention periods for images and access to images (including sharing with a third party)- areas which	Surveillance camera systems are operated unlawfully, inconsistently or inefficiently.	High	A single corporate policy on use of surveillance camera systems will be developed covering their use on both buildings and vehicles. A process will be developed to ensure that digital images recorded on surveillance cameras can be retrieved, transferred and stored in a secure and effective manner.

	have been identified as lacking documentation over the course of this audit.			
Responsible Officer:		Information Security & Data Protection Officer	**Target Implementation Date:**	30/09/2022 (includes full consultation process)

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
2	**Statements of need/DPIAs** Principle 1 of the Surveillance Camera Code of Practice states: *Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.* For a sample of three surveillance camera systems on buildings, a Privacy Impact Assessment (PIA) could be provided for one. Whilst the PIA does cover why there is a need for CCTV, it was completed in 2015 and has not been updated since. This date is prior to the requirement for a Data Protection Impact Assessment (DPIA) to be completed (this was introduced in 2018 as part of GDPR legislation). However, good practice would be to conduct a DPIA for this system to formally document information such as the current lawful bases for the system, and to capture any changes since the system's implementation. For the other two surveillance camera systems on buildings, no written statement	ESFRS could be in breach of data protection laws if it cannot evidence the objective of its surveillance camera systems and the lawful bases by which they are deployed. This could result in fines from the Information Commissioner's Office	High	A process for the completion of DPIAs for surveillance cameras will be put in place along with template DPIAs. The process will be owned corporately. DPIAs for existing cameras will be completed by the Estates Team and Engineering Team. Future DPIAs will be completed by the Estates Team and Engineering Team before additional surveillance cameras are deployed.

	of need could be provided. A DPIA is in place in relation to the use of surveillance cameras on vehicles. However, this does not explicitly outline which of the 6 lawful bases the cameras have been deployed under. For the surveillance camera systems we have sampled, therefore, there is insufficient documented evidence as to the need for the cameras, and the lawful bases for their deployment.			
Responsible Officer:		Corporate DPIA process: Information Security & Data Protection Officer Estates: Major Capital Projects Manager Engineering: Engineering Services Manager	**Target Implementation Date:**	30/04/2022 for existing cameras 30/09/2022 for new policy and templates

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
3	**Governance Arrangements** Principle 4 of the Surveillance Camera Code of Practice states: *There must be clear responsibility and accountability for all surveillance camera system activities*. To facilitate this, the Surveillance Camera Commissioner also encourages nominating a Single Point of Contact (SPoC) to oversee all surveillance camera systems and ensure they are compliant with the Surveillance Camera Code. ESFRS does not currently have a nominated SPoC, and responsibility for cameras sits over a number of different teams including Estates and Engineering, with no holistic overview as to how the authority complies with the Surveillance Camera Code. Roles and responsibilities are also not formally documented, and therefore cannot currently be fully understood or adhered to by all staff.	Surveillance camera systems are operated unlawfully, inconsistently or inefficiently.	Medium	The Single Point of Contact (SPOC) will be the Information Security & Data Protection Officer (IS&DPO). Responsibility for compliance in relation to buildings and vehicles will rest with the Senior Estates Surveyor and the Engineering Services Manager respectively. The roles and responsibilities of both the SPOC and the departmental compliance officers will be set out in the corporate policy on the use of surveillance camera systems (see R1)
Responsible Officer:	Information Security & Data Protection Officer	**Target Implementation Date:**	30/09/2022	

Ref	Finding	Potential Risk Implication	Risk	Agreed Action	
4	**Signage** Appropriate signage was in place for the majority of our sample of surveillance camera systems. This is necessary to inform individuals that they are being monitored. However, no such signage was in place at Preston Circus. At this location, cameras face the entrance gates so may capture members of the public. Additionally, no signage was found to be present on any vehicles fitted with surveillance cameras, which may also capture members of the public.	Members of the public may not have been aware of the CCTV cameras in the location and unable to consent due to lack of transparency.	Medium	The requirement and standards for signage will be set out in the corporate policy on the use of surveillance camera systems. Estates: Action already implemented- signage installed at Preston Circus. Engineering: Signage to be designed and fitted to vehicles already fitted with CCTV	
Responsible Officer:		Policy: Information Security & Data Protection Officer Engineering: Engineering Services Manager	**Target Implementation Date:**		Policy by 30/09/2022 Existing vehicles fitted with surveillance cameras by 31/03/2022

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
5	**Privacy notice** A privacy notice is available to the public on the ESFRS website, and makes refence to CCTV, stating: *We...process personal information using a CCTV system to monitor and collect visual images for the purpose of security and the prevention and detection of crime.* It also contains contact details for the authority's Data Protection Officer. However, this is the full extent of information on surveillance cameras included in the Privacy Notice, and on the wider ESFRS website. Good practice would be to have more in depth information, or indeed, a separate notice relating to surveillance cameras.	Members of the public are not aware of how ESFRS use surveillance cameras and are unable to consent due to lack of transparency.	Low	Information provided on the Service's website will be updated to reflect good practice and a link provided to the Service's policy of the use of surveillance camera systems.
Responsible Officer:		Information Security & Data Protection Officer	**Target Implementation Date:**	31/10/2022

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
6	**Insurance Requirements** The authority's vehicle insurers offer a discount where surveillance cameras are present on vehicles and meet a number of requirements. ESFRS has been found not to qualify for such a discount. This is due to a lack of direct access to images from cameras- whilst the SD card can be accessed, the images on this cannot be viewed by ESFRS or fully utilised. Also, it is noted that if more vehicles were fitted with cameras (with accessible and usable images), any discount received on the insurance would be greater.	Failure to reduce insurance costs and improve insurance claims performance- value for money is not realised	Low	A business case is being developed for the installation of CCTV on both heavy and light fleet, alongside a joint procurement exercise with WSCC. The business case will be submitted for approval in sufficient time to allow installation on at least part of the fleet before the renewal of our insurance November 2022.
Responsible Officer:		Engineering Services Manager	**Target Implementation Date:**	30/06/2022

Appendix A

Audit Opinions and Definitions

Opinion	Definition
Substantial Assurance	Controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Reasonable Assurance	Most controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Partial Assurance	There are weaknesses in the system of control and/or the level of non-compliance is such as to put the achievement of the system or service objectives at risk.
Minimal Assurance	Controls are generally weak or non-existent, leaving the system open to the risk of significant error or fraud. There is a high risk to the ability of the system/service to meet its objectives.

Management Responsibilities

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

This report, and our work, should not be taken as a substitute for management's responsibilities for the application of sound business practices. We emphasise that it is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal Audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.