Loss Prevention Standards – Asset Classes

Video Surveillance Systems - Introduction

Version: 1.2
Date: 21st March 2025

Video Surveillance Systems (VSS), formerly known as Closed-Circuit Television Systems (CCTV), help provide enhanced premises security, often acting as a deterrent to criminal activity.

This Loss Prevention Standard provides an overview of the technology and guidance on the effective use and management of VSS.

AVIVA

Video Surveillance Systems - Introduction

Introduction

Video Surveillance Systems (VSS) are an effective and versatile tool that can help prevent or reduce criminal activity and anti-social behaviour, achieving this by a combination of:

- Deterrence.
- Detection/response.
- Provision of evidence.

VSS should be part of an overall security strategy and used in conjunction with other security equipment and systems, such as window and door locks, security barriers, intruder and hold up alarm systems etc., to provide consolidated premise security protection.

Whilst originally an expensive security measure, technological developments and reducing costs, coupled with greater versatility and reliability in recent years has led to such systems becoming commonly used across towns, cities, industrial parks and individual business premises.

This Loss Prevention Standard provides general guidance on choosing the most effective Video Surveillance System.

VSS Components

VSS typically comprise the following main components:

Cameras. Modern systems generally use digital camera equipment which provides enhanced functionality over the traditional analogue equipment, such as internet connectivity which allows streaming of footage to devices; megapixel resolution; motion detection; target tracking; pan-tilt-zoom (PTZ); light manipulation etc. Specialised camera equipment can also be used to record thermal images, which may be useful for premises or locations with low to zero overnight occupancy.

Detector Devices. Whilst most VSS will be capturing images and recording constantly, some systems are triggered by detection devices. Common types includes motion detectors which detect movement in the cameras range and infrared detectors which detect heat signatures and are often used in low light situations.

Recording Devices. Modern systems typically utilise Network Video Recorders (NVRs) to store the footage captured by the cameras.

Monitors. Monitors are used to display the live or recorded video images from the site cameras.

The equipment will also generally include networking equipment e.g. cabling, routers etc., along with software products to enhance the recording and viewing experience and capability.

Whilst a basic VSS may act as a general deterrent to crime, unless it is being observed continuously, it is only able to provide recorded evidence of events discovered or suspected after they have actually occurred. If a VSS is to play a pro-active security function, it is usually necessary for the system to be activated by some form of alarm detector, which then initiates the live transmission of images to an occupied monitoring post e.g., a security lodge/gatehouse or a third party managed Remote Video Response Centre (RVRC). Such monitoring allows security operatives to view events as they unfold and provide an immediate and appropriate response.

Common Applications for VSS

VSS can be used in many situations, including the following:

Access Control

- Checking identity of persons seeking entry.
- Monitoring access to car parks or private roads.

Monitoring Safety

- In public areas.
- Staff working in vulnerable occupations or locations.
- Customers.

Controlling Theft, Arson and Vandalism

By monitoring:

- Cash handling positions.
- Bank vaults or similar high-security areas.
- Unoccupied areas such as warehouses, goods' loading bays and yards.
- Activities of workers/the public.
- Shoplifters.
- Premises and yards outside normal business hours.

VSS can also manage response strategies in support of installed Intruder Alarm and Hold Up (I&HAS) system activations by providing visual evidence of the activation cause to another location, such as an RVRC, as well as providing data to support analysis and defensibility.

Choosing a VSS

Prior to choosing/purchasing a VSS, a security risk assessment should be completed to fully understand:

- Gaps or omissions in the site management such as ownership, co-ordination, and communication issues etc.
- The vulnerable assets at the site.
- The likelihood of a theft incident occurring based on local knowledge, local crime data, sector trends including local police response to incidents.
- The likely extent of any intruder related damage.
- The impacts to site activities and site profitability.
- The adequacy of current security arrangements.
- How site occupancy impacts the security exposures.
- Gaps in security knowledge.
- Security review arrangements.
- Cyber security measures.
- Necessary improvements to the security arrangements.

The risk assessment should be undertaken and reviewed by persons with a working knowledge of the premises and its vulnerabilities, good knowledge of the locality and any recent or ongoing local theft or malicious activity. A reputable security company or a Security Consultant, preferably one registered with the Register of Chartered Security Professionals, can assist with security risk assessments and choosing the most appropriate system type and specification.

Important: Discuss any planned security protection changes with your Property Insurer and Broker, who can also provide guidance on VSS security systems.

The most effective VSS is likely to be a detector activated system, monitored by an accredited RVRC, and achieving level 1 police response. This ensures any activations can be actioned immediately and appropriately.

To achieve level 1 police response, the system will need to be installed, maintained, and monitored to the requirements of BS8418: Design, installation, commissioning and maintenance of detection-activated video surveillance systems (VSS). Code of practice and be issued with a Unique Reference Number (URN) by the local Police force.

A police response to VSS activations may not be necessary for all systems, particularly if an on-site or contracted security guard response is provided, or the premises are located in a remote area where police response cannot be delivered within a meaningful timescale.

To help improve the deterrent value of such a system, the incorporation of an audio challenge facility, which allows the RVRC to issue warnings to any unauthorised persons attempting to access the site or behaving suspiciously, should be considered. In areas with high crime rates, or sites that have suffered previous or recent security concerns or incidents, the VSS can be extended to include Automatic Number Plate Recognition (ANPR) equipment to capture and record the registration details of vehicles entering the premises grounds.

Installation of a VSS

To ensure the best quality of service, the Installer and RVRC should be members of a UKAS third-party accreditation/approval scheme, such as those provided by the National Security Inspectorate (NSI) or Security Systems and Alarms Inspection Board (SSAIB). This is a requirement for any VSS requiring a police response.

These companies are fully audited against British/European Standards for:

- System design.
- Installation.
- Maintenance.
- Monitoring.
- Staff security vetting, training and record keeping.

Note: Clear, readable signage should be displayed on the premises warning individuals that VSS surveillance is operational. The presence of such signage in prominent locations such as entrance gates, perimeter fencing and near critical equipment and buildings can be a significant deterrent to intruders. Emergency contact numbers should also be provided for persons wishing to report any security concerns.

Responding to a VSS Activation

Wherever a VSS is monitored, it is important that clear requirements and procedures are put in place for those persons expected to respond, for example:

Locally Monitored Systems

Individuals and employees will need specific training in the correct use of the system, and the standard operating procedure for dealing with persons pursuing any criminal acts or trespassing etc.

Note: Staff keyholding and site response to VSS detection alerts is not recommended, unless in accompaniment of approved security guarding or the police.

Remotely Monitored Systems

Clear instructions are typically detailed in a formal 'Response/Escalation Plan' or 'Service Agreement' outlining the actions that are required following any activation or signal fault.

These actions should cover notifying the police; security personnel; keyholders; building maintenance engineers; the site emergency response team or any combination of these. Those who attend site should:

- Know how to operate all the site security systems.
- Have the authority to expedite essential repairs.
- Be prepared to remain at the premises until adequate security has been restored. This latter point should be detailed formally in any site Emergency Response Plan.

Police Response

RVRCs dealing with remotely monitored VSS systems can quickly and reliably request police attendance. However, as discussed earlier in this standard, this is only if the:

- System has been issued with a Unique Reference Number (URN) by the local police force.
- VSS meets the requirements of **BS 8418: Design, installation, commissioning and maintenance of detection-activated video surveillance systems (VSS). Code of practice** and the installer and RVRC hold National Security Inspectorate (NSI) or Security Systems and Alarms Inspection Board (SSAIB) approval.

The police are generally supportive of VSS as a means of combating crime. However, if they are to act directly on live or captured images, they have to be able to satisfy themselves that they come from systems that meet high standards of operation, image quality and evidential procedures. In this regard, useful documents for VSS owners/purchasers to review are:

- UK Police Requirements for Digital VSS Systems
- Code of Practice from the Surveillance Camera Commissioner

Security Company Response

Given the remote nature of many PV/Solar Farms, and anticipated delays in police response in some localities, it may be more appropriate to utilise a security company to provide keyholder and VSS detection response services, rather than rely on police response. Regular security patrols of the site by the security company can also provide a significant deterrent to intruders.

Any such providers should be members of the Security Industry Authority and provide their services in accordance with the requirements of **BS 7984-3:2020 Keyholding and Response Services - Provision of Mobile Security Services. Code of Practice.** They should also be members of a UKAS third-party accreditation scheme, such as those provided by the National Security Inspectorate (NSI), or the Security Systems and Alarms Inspection Board (SSAIB).

The Private Security Industry Act 2001 requires contracted security guards, VSS response personnel and those who monitor VSS covering public spaces, to hold an SIA licence.

Data Protection – General Data Protection Regulation (GDPR)

The GDPR requires most VSS to be registered with the Information Commissioner's Office (ICO). This requirement arises because nearly all VSS include a method of recording and storing images from the cameras. This regulation also gives members of the public a right to ask for copies of any data about them held on such systems.

Additional legislation which applies to CCTV systems include the Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice 2013.

Cyber Security

Cyber security exposures should be reviewed for 'connected VSS' to ensure appropriate protections and procedures are incorporated including data access approval management.

Aviva Loss Prevention Standards **12 Top Tips to Protect Against Cyber Attacks, Cyber – Ransomware, Cyber Incident Response Process** and **Cyber Essentials Accreditation** provide further guidance.

Checklist

A generic **VSS Checklist** is presented in Appendix 1 which can be tailored to your own organisation.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

Electronic Security Services - **Secom**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- British Security Industry Association (BSIA)
- UK.GOV – Local Councils: Crime Prevention and Community Safety
- RISCAuthority – S20: Essential Principles for the Security of Property
- RISCAuthority – S23: Guidance for Specifiers of VSS in Security Applications
- BS EN 62676 – Video Surveillance Systems for use in Security Applications
- BS8418: Design, installation, commissioning and maintenance of detection-activated video surveillance systems (VSS). Code of practice
- BS 7984-3: Keyholding and Response Services - Provision of Mobile Security Services. Code of Practice

Additional Information

Relevant Loss Prevention Standards include:

- **Intruder and Hold Up Alarms – General Guidance**
- **Intruder Alarms European Standard**
- **12 Top Tips to Protect Against Cyber Attacks**
- **Cyber – Ransomware, Cyber Incident Response Process**
- **Cyber Essentials Accreditation**

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Appendix 1 – VSS Checklist

Location	
Date	
Completed by (name and signature)	

	VSS: General Guidance	Y/N	Comments
1.	Has a security risk assessment been undertaken of the current security systems and measures in place at your premises? Does this include the following: • Local history of security related events? • Nature of building contents/occupancy, especially close to each window/door and its attractiveness to theft? • Accessibility of the area for criminals? • Provision of anything that could improve access to upper levels/roof of the building? • Strength and nature of the building construction in comparison to any doors/windows and securing mechanisms? • Nature of any physical barriers, such as fences? • The nature of any other electronic security measures or human presence on site? • Management systems and escalation plans?		
2.	Has independent crime prevention advice been sought from: • The police? • A security consultant? • Your insurer(s) and Broker?		
3.	• As part of your security assessment, have you considered to what extent VSS will address any risks or exposures? • Have you considered how other security measures will complement the VSS and vice versa, e.g. improved physical security or an intruder alarm system?		

	VSS: General Guidance Contd.	Y/N	Comments
4.	• Have you used a reputable and competent VSS supplier? • Is this company listed by the National Security Inspectorate (NSI) or Security Systems and Alarms Inspection Board (SSAIB)?		
5.	• Have any potential interested parties, e.g. employees, tenants, local residents, etc., been informed of your VSS use or your intention to use a VSS system? • Are clearly readable signs displayed to advise individuals that a VSS is operational, and recording is taking place?		
6.	• Have you considered what employee training is or will be needed? • Does this include refresher training?		
7.	Are there clear procedures in place for those viewing or having access to the images created by the VSS?		
8.	• Are the images from the VSS recorded locally? • If so, are there clear procedures in place for those having access to these recordings?		
9.	• Does the VSS have any associated monitoring? If so, Is this: ✓ Local? ✓ Remote? ✓ Contracted-out/Service Provider? • Are there any associated alarms with this arrangement that indicate any issues with the transmission of these images? • Is there a Service Level Agreement and formal escalation plan?		

	VSS: General Guidance Contd.	Y/N	Comments
10.	Has the Emergency Response Plan been provided/revised to consider an event unfolding and captured on the VSS? • Is the level of response appropriate and consummate with the risk? • Are notification and escalation plans in place with appropriate officials and personnel identified to respond to an incident? • Are the local police included in this escalation plan? • Has this plan been tested? • Is this plan reviewed periodically and revised accordingly?		
11.	Have you checked whether or not you need to register your VSS with the Information Commissioner's Office (ICO)?		
12.	Do you have procedures in place to cover the vulnerability of the site if there is any impairment or compromise to the VSS or, if provided, its remote transmission?		
13.	Have you reviewed cyber security arrangements and extended adequate protection to the VSS?		
14.	Are security arrangements and the basis for the security risk assessment regularly reviewed, including following any security issues, local incidents, intrusions or losses? **Note:** If not, you are likely to be at more risk of a repeat incident.		
15.	Additional comments:		

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

21st March 2025

Version 1.2

ARMSGI1402020