Planning, design, installation and operation of Video Surveillance Systems (VSS)

Code of practice and associated guidance

THE VOICE OF THE **PROFESSIONAL SECURITY INDUSTRY**

bsia
british security industry association

Document conventions

Text shown in this style forms the code of practice section of this document.

Text shown in this style forms the associated guidance to help the readers understand the code of practice.

Contents

1. Introduction

Video Surveillance Systems (VSS) are frequently the subject of debate. Some parties seek to promote their benefits such as their use in criminal investigations and providing a feeling of safety to the public. They have also been on the receiving end of bad press when some consider their right to privacy has outweighed the safety and security benefits.

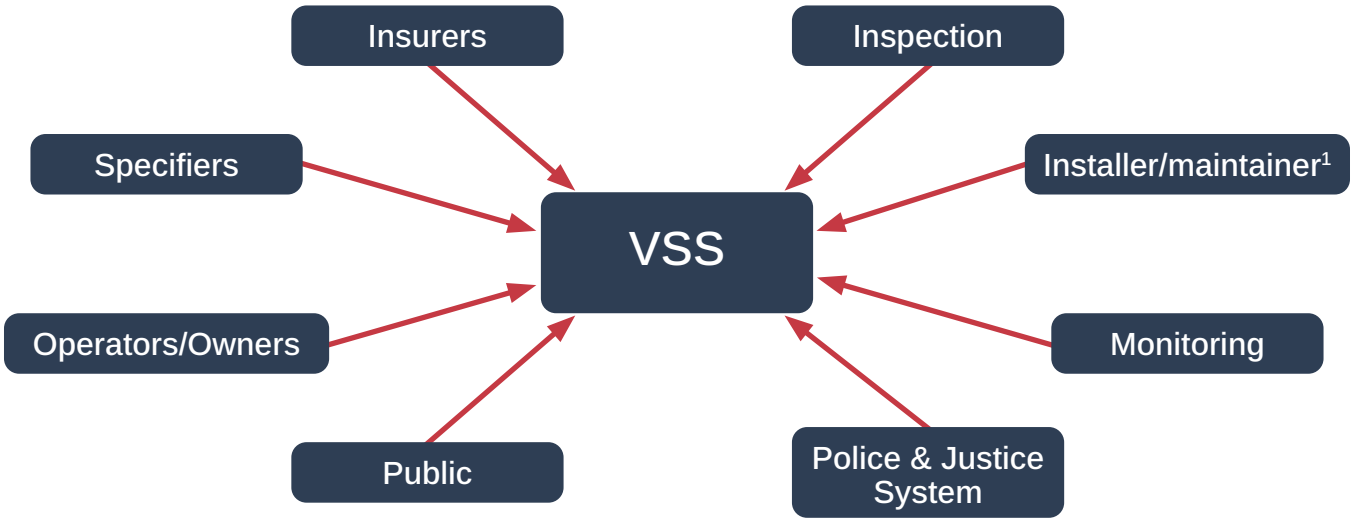
The correct design and use of such systems is paramount to ensure that a VSS system meets the needs of the user, provides a tangible benefit and provides safety and security for the general public.

This code of practice has been prepared to assist in this process by taking account of the various standards for VSS and presenting them in a useable framework showing the "building blocks" necessary to achieve an effective security surveillance solution.

It is important to remember the significance of cybersecurity in VSS design and installation. Not all VSS have a cyber exposure but for those systems that do, it is vitally important to ensure that this is mitigated effectively. For further information on cybersecurity, see BSIA Form 342 Installation of safety and security systems - Cybersecurity code of practice and BSIA Form 343 Manufacturers of safety and security systems - Cybersecurity code of practice.

This document will be of use to many key stakeholders, all of which need to be considered at the planning and design stages, such as those shown in Figure 1:

Figure 1: Key stakeholders for video surveillance



[1]Recommendations for maintenance can be found in BSIA Form 120.

In the UK, the Home Office and the Scottish Government have recognised the potential for appropriate and effective use of VSS. There is regulation included in the Protection of Freedoms Act. One of its legislative requirements is the development of the Surveillance Camera Commissioner's Code of Practice, to which this document shares the same goal. For Scotland, the Scottish Government published A National Strategy for Public Space in Scotland which includes a standards and regulatory framework. Cross references to the 12 Guiding principles of the Home Office Surveillance Camera Code of Practice (SCCoP) are shown in boxes at the start of relevant sections.

In this document, reference is made to both European (CENELEC) and International (IEC) Standards that introduce the concept of "grading" of VSS. Grading is considered to be risk dependant, which may differ for certain parts of a VSS, therefore introducing the possibility of having different grades within one VSS[2]. Therefore, grading need not feature in a VSS unless specified in its operational requirement.

[2]Further guidance on VSS grading has been published in BSIA Forms 217 and 218.

2. Scope

This code of practice gives recommendations for the planning, design, installation and operation of all VSS when utilised for safety and/or security. Its content takes into account the work undertaken by both the International Electrotechnical Committee (IEC), European committee for electrotechnical standardisation (CENELEC) and British Standards Institution (BSI).

The content of this code of practice should assist with compliance with the Surveillance Camera Code of Practice (published by the Home Office). Recommendations for maintenance of VSS are outside the scope of this code of practice and can be found in BSIA Form 120.

3. Reference standards and documents

SCCoP Guiding Principles (see ANNEX C)	**Principle 8 states:** Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards

The following referenced standards and documents will assist in application of this code of practice.

Note: The 62676 series of standards were developed by the IEC as international standards but published in the UK as BS EN or BS EN IEC standards. You may see references to these as "IEC standards". This lists of standards and other references below were correct at the time of the publishing of this code of practice.

3.1. Standards

BS EN 62676 series	Video surveillance systems for use in security applications
BS EN 62676-1-1	System requirements - General
BS EN 62676-1-2	System requirements - Performance requirements for video transmission
BS EN 62676-2-1	Video transmission protocols – General requirements
BS EN 62676-2-2	Video transmission protocols – IP interoperability implementation based on HTTP and REST services
BS EN 62676-2-3	Video transmission protocols – IP interoperability implementation based on web services
BS EN 62676-3	Analog and digital video Interfaces
BS EN 62676-4	Application guidelines
BS EN IEC 62676-5	Data specifications and image quality performance for camera devices
BS EN IEC 62676-2-31	Live streaming and control based on web services
BS EN IEC 62676-2-32	Recording control and replay based on web services
BS EN 60529	Degrees of protection provided by enclosures (IP Code)
BS EN 62305 series	Protection against lightning
BS EN ISO 11064 series	Ergonomic design of control centres
BS 5979	Remote centres receiving signals from fire and security systems. Code of practice
BS 7671	Requirements for electrical installations. IET wiring regulations.
BS 7958	CCTV Management and Operation – Code of Practice
BS 8418	Design, installation, commissioning and maintenance of detection-activated video surveillance systems (VSS). Code of practice

BS EN 50518	Monitoring and alarm receiving centre
BS 8591	Remote centres receiving signals from alarm systems – code of practice
BS 9518	Processing of alarm signals by an alarm receiving centre - Code of practice
BS 10008-1	Evidential weight and legal admissibility of electronically stored information (ESI).Specification
BS 10008-2	ESI - Code of practice for implementation of BS 10008-1
BIP 0009	ESI - Compliance checklist for use with BS 10008-1

3.2. Other references

PSDB 09/05	HOSDB/ACPO UK Police requirements for digital CCTV systems
HO 28/09	HOSDB - CCTV operational requirements manual 2009
HO 66/08	HOSDB - Retrieval of video evidence and production of working copies from digital CCTV systems v2.0
HO 58/07	HOSDB digital imaging procedure
BSIA Form 120	Maintenance of Video Surveillance Systems (VSS) - code of practice
BSIA Form 197	CCTV privacy masking guide
BSIA Form 199	VSS chip and PIN guide
BSIA Form 217	Guidance for customers about grading and other important matters
BSIA Form 218	Graded requirements under BS EN 62676 Standards for CCTV
BSIA Form 342	Installation of safety and security systems - Cybersecurity code of practice
BSIA Form 343	Manufacturers of safety and security systems - Cybersecurity code of practice
BSIA Form 347	Automated Facial Recognition - A guide to ethical and legal use

4. Definitions and abbreviations

4.1. Definitions

4.1.1. VSS

System consisting of camera equipment, storage, monitoring and associated equipment for transmission and controlling purposes.

Note: In this context, the term VSS are synonymous with CCTV systems.

4.1.2. Security company

An organisation that provides a service for the design, installation, commissioning, maintenance or monitoring of VSS.

Note: The term security company is used within this document to refer to an organisation providing any or all of these services to a system owner. Depending on the business arrangement the security company and the owner could be the same organisation. Alternatively, the monitoring and operation of the system may be performed by the owner or another organisation (e.g. a security company).

4.1.3 Surveillance

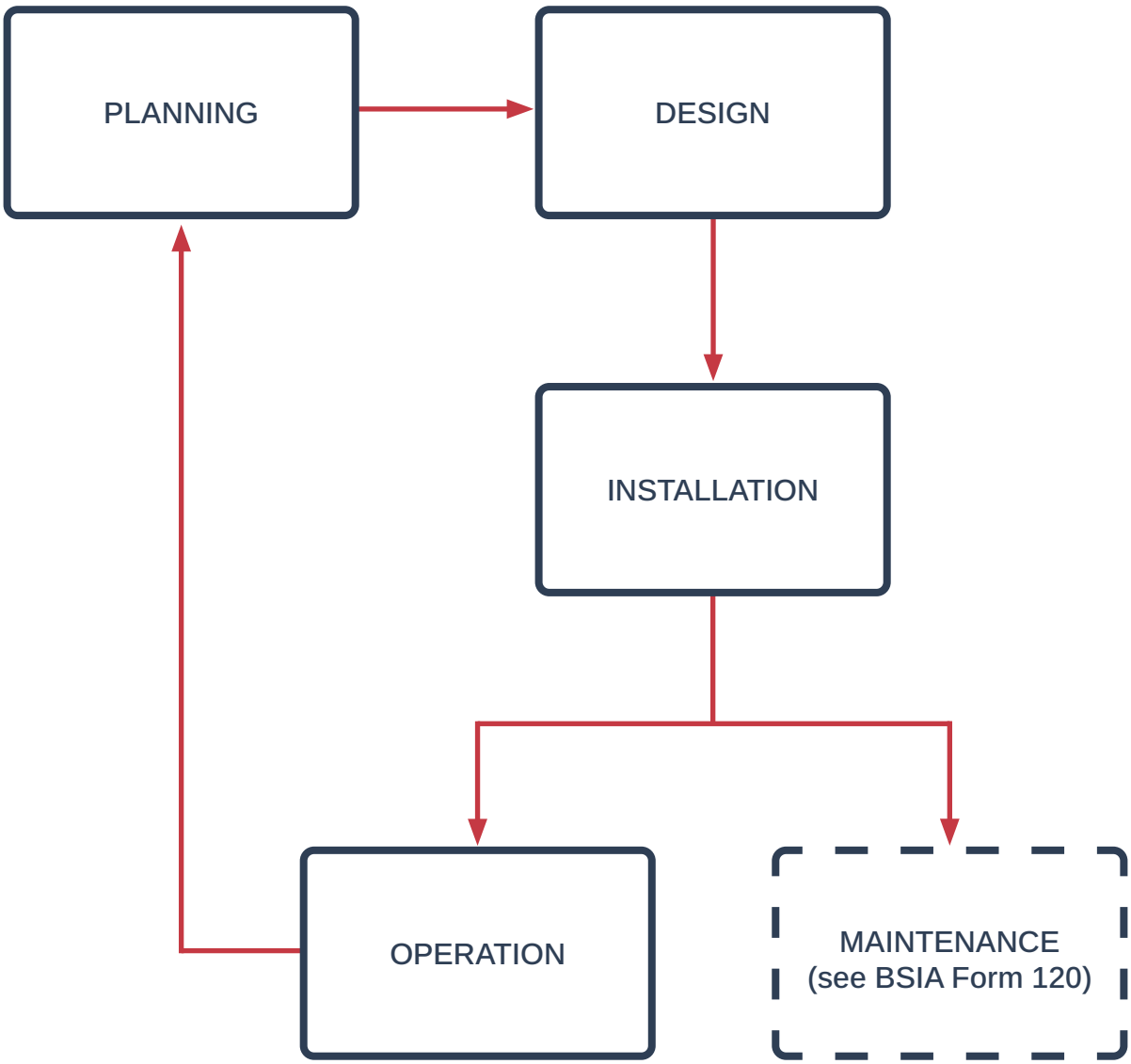
Observation or inspection of persons or premises for security purposes

4.2. Abbreviations

The following abbreviations appear in this code of practice:

ATEX	Explosive Atmospheres (from ATmosphères EXplosives)
AFR	Automated Facial Recognition
ANPR	Automatic Number Plate Recognition
BS	British Standard
BSI	British Standards Institution
BSIA	British Security Industry Association
CAST	Centre for Applied Science and Technology (Home Office)
CCTV	Closed Circuit Television
CENELEC	Comité Européen de Normalisation Électrotechnique; (European Committee for Electrotechnical Standardization)
DPA	Data Protection Act
EN	European Standard
FAT	Factory Acceptance Test
HD	High Definition
HOSDB	Home Office Scientific Development Branch (former name of CAST)
IEC	International Electrotechnical Committee (Worldwide standards body)
IP	Internet Protocol or Ingress Protection Rating (according to context)
ISO	International Standards Organisation
ONVIF	Open Network Video Interface Forum
OR	Operational Requirement
PAL	Phase Alternating Line (TV encoding system)
PoE	Power over Ethernet
PSIA	Physical Security Interoperability Alliance
PTZ	Pan-Tilt-Zoom
PVC	Polyvinyl Chloride
RAID	Redundant Array of Independent Disks
RVRC	Remote Video Response Centre
SCCoP	Surveillance Camera Code of Practice
SCC	Surveillance Camera Commissioner
SDP	System Design Proposal
SXGA+	Super Extended Graphics Array Plus
TX	Transmission

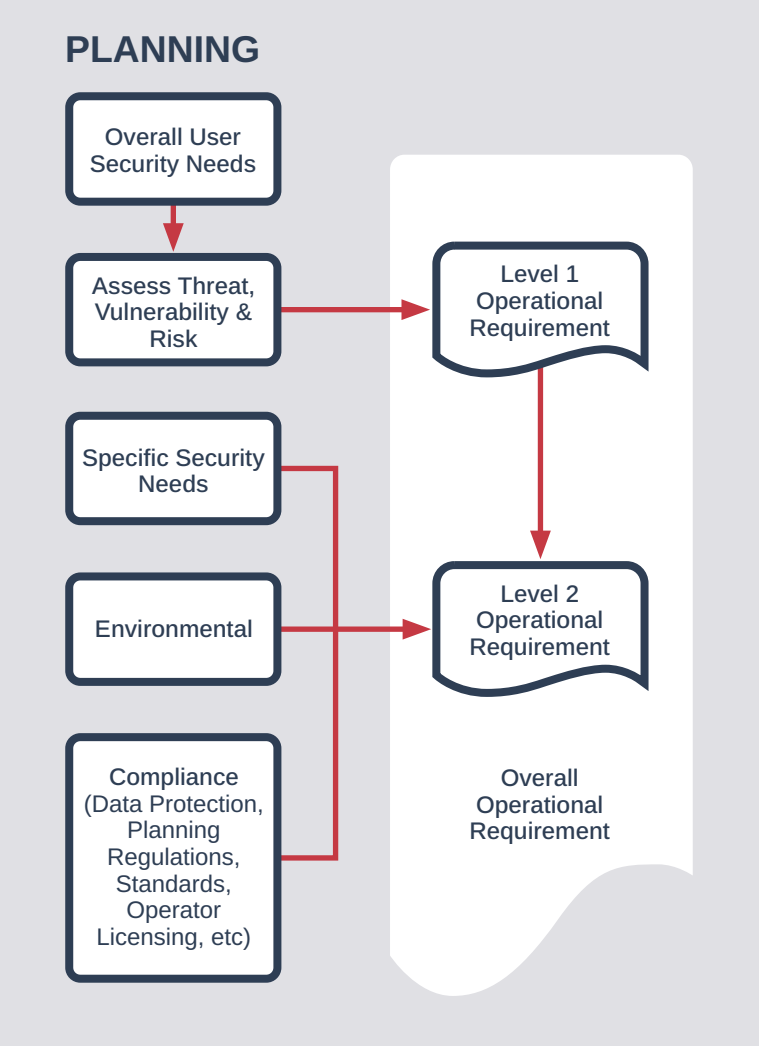
5. Flowchart



6. Planning

6.1. Flowchart

The use of an Operational Requirement (OR) (see 6.4) is usually recommended although the form of this may vary. For simple systems, the OR may be developed in a single iteration but for complex systems it may require a cycle of development. The following flowchart suggests that it may be preferable to consider the overall needs of the user and to agree these before considering more specific needs in consultation with the supplier of the system.



6.2. Capturing user need

SCCoP Guiding Principles (see ANNEX C)	**Principle 1 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.

It is the responsibility of the system specifier or purchaser to identify and record the purpose of the VSS. The security company should ensure that the fundamental reasons for the system are recorded in the OR or System Design Proposal (SDP). To enable effective planning of an installation and to ensure that the design outcomes yield a suitable solution, the security company should capture as much pertinent information as possible from the client.

When planning VSS it is important to remember that there is no 'one size fits all' solution. Each site will have its own unique needs based around numerous factors (including nature of site, geographic location, local environment, history of issues). Similarly, each end user will likely have their own expectations regarding how the system will complement their overall security solution (e.g. deter crime, improve detection of crime, monitoring movement of personnel).

Nobody is likely to know the needs and expectations as well as the local prospective user(s) of the system and therefore it is important to engage them to draw on their concerns, experiences and expectations of the system. This will help build a fuller picture for the subsequent planning elements outlined below.

6.3. Threat, vulnerability, risk assessment

A threat, vulnerability and risk assessment should be performed to ensure that the design of the system adequately addresses or mitigates the threats, vulnerabilities and security risks. The result of this activity should be recorded in a suitable manner and may form part of an operational requirement or system design proposal but in some cases the system owner may prefer to restrict access to the full assessment and provide only the conclusions to the security company.

It is important to ensure that any VSS / security measures installed are effective in mitigating the threats, vulnerabilities and risks present. In order to identify the level(s) of security required (and potentially therefore the grading of the elements of the system), an assessment of the factors which are likely to come into play is required.

Numerous definitions and calculations for threat, vulnerability and risk exist, often industry or application specific (e.g. building sites etc) and are often based around health & safety. In very global terms, from a security perspective these elements are typically considered as:

***Threat (Who):** The threat will typically be defined as the persons or events to be protected against. Threats will vary greatly in terms of objectives, determination, capability, resourcefulness, etc. and may include:*

***Opportunist Thief:** e.g. petty shoplifter. Often unplanned / non pre-meditated. Relatively low skill set. Typically non-violent.*
***'Professional' Thief:** Planned, targeted theft. Medium skill set. Typically non-violent.*
***Organised Crime:** Planned / targeted. High skill set. May be violent.*
***Single Issue Groups:** Examples include animal rights activists, environmental activists. Planned, targeted attacks / events. Typically highly skilled and highly determined. Often non- violent (although may actively resist arrest).*
On a wider perspective, threats may also be defined as non-specific / non targeted such as environmental conditions (e.g. flood monitoring).
***Terrorism:** Planned / targeted. Moderate skill set. Likely to cause maximum damage to life safety.*

***Vulnerability (What / Where):** The vulnerability will typically be the areas of concern that require protection. The level of vulnerability will be defined by numerous factors such as desirability of the objects in the area, ease of access, operational hours of the environment, exposure / secluded nature of the area. These factors need to be cross referenced against the identified threats as the vulnerability level will differ for each threat based on their perceived nature such as determination and skill sets– e.g. an opportunist may be put off by a locked lightweight door that an organised crime group may smash down.*

***Risk (What if?):** Risk is effectively the consequence of a successful or attempted intrusion or event. These risks can be wide and varied and not immediately obvious. Risks and impact levels of each identified risk will typically vary depending on the nature of site. Risks can include:*

***Immediate Financial Loss:** Immediate value of items lost.*
***Ongoing Financial Loss:** Increased insurance premiums, time to return to profit.*
***Personal Safety:** Injuries to staff and / or members of public involved in violent incident.*
***Stress Related Issues:** Reduced staff morale, loss of staff due to safety concerns.*
***Non-financial loss:** May include loss of intellectual property, data or similar.*

Typically, security systems cannot change the identified threats or vulnerabilities, but well deployed security measures significantly reduce the likelihood of an intrusion or event, which in turn will help to reduce the risk.

Cross sections of the above threat, vulnerability and risk factors, once identified, should be used to define the specification or grading levels of equipment to be utilised. For example, situations perceived as low skilled, low determination threats in areas of limited vulnerability and little or no risk may require Grade 1, whilst areas identified as high threat with high vulnerability and high risk may require Grade 4.

6.4.Establishing operational requirements and agreeing with the customer

Operational requirements should be documented to clearly define the needs and expectations of the VSS and its relevance to the threat, vulnerability and risk assessment above as well as capturing the user needs.

The OR document (or the operations requirements section of a system design proposal, if not a separate document) should include the following information:

- Definitions of areas under surveillance
- Limitations of surveillance
  - This may include any local legislations or privacy issues
- Activity to be captured
  - Definition of targets
  - Observation category of target (e.g. detect, recognise, identify – see 6.5)
- Image/picture performance
  - e.g. level of detail operator to be able to perceive
- Periods of anticipated operation/usage
- Site Conditions
  - Specific issues which may affect camera views such as fog, large vehicle movement, lighting conditions
- Resilience – i.e. need for backup power supplies, cybersecurity etc.
- Video image storage and monitoring requirements
  - Image recording rates for normal and event periods
  - Retention period & deletion (how long images should be stored for)
  - Where and who should be able to monitor images
- Extracting/Exporting images
  - Procedures
  - Who and where this can be carried out
  - Media to be extracted to
  - Likely periods/quantity of data to be exported
- Operational response
  - Persons responsible for responding
  - Response procedures
  - Response times
- Training
  - Definition of training required for different elements of the system, e.g. routine monitoring, image export etc.
  - Quantities of persons requiring training
- Planned or possible future expansions to the system, including addition of further cameras, monitoring locations and integration with other systems.
- Where there is a need to use additional technology, e.g. AFR, ANPR

Ideally the OR document should be raised by the end-user or their authorised representative (such as a security consultant) and used as the basis for specifying the required system and subsequent performance tests. However, the operational requirements may also form a part of a SDP provided to the end-user as a statement of identified needs.

6.5. Target capture and image detail

It is important to consider the level of detail required in an image so that it matches the need of the user. This should be discussed with the client. The practical effect of this is that a camera may need to have a wider or narrower field of view so that the necessary amount of detail can be seen and in some circumstances more cameras may be needed, either to increase the area covered with the same detail or to allow for different levels of detail to be seen from the same view.

Whether the different levels of detail can be achieved using a single PTZ or single camera of high resolution is a matter that should be agreed.

The typical levels of detail are shown in table 1. See Annex E of BS EN 62676-4 for further information.

Table 1: Levels of image detail

Purpose	Description (Equivalant pixels/m at target distance)	Relative view (The dashed lines represent the top of a viewing screen)
Monitor	*To enable viewing of the number, direction and speed of movement of people across a wide area, providing their presence is known to the operator.* *12.5 pixels/m*	
Detect	*To enable the operator to reliably and easily determine whether or not any target (e.g. a person or vehicle) is present.* *25 pixels/m*	

Purpose	Description (Equivalant pixels/m at target distance)	Relative view (The dashed lines represent the top of a viewing screen)
Observe	*To enable characteristic details of an individual, such as distinctive clothing to be seen, whilst allowing a view of activity surrounding an incident.* *62.5 pixels/m*	
Recognise	*To enable the operator to determine with a high degree of certainty whether or not an individual shown is the same as someone they have seen before.* *125 pixels/m*	
Identity	*To enable identification of an individual beyond reasonable doubt.* *250 pixels/m*	
Inspect	*To enable information to be obtained from objects in the image, e.g. read text or a logo on clothing* *1000 pixels/m*	

Note that these stated image sizes are based on PAL (Analogue) or 4CIF (Digital) resolution images and are typical minimums for these resolutions. Other recommended minimums for higher resolution systems may be found in Annex E of this document and full details for many commonly used resolutions are described in table 3 within section 6.7 of BS EN 62676-4.

Account should also be made of the difference between live operation and playback / review operation when considering image size requirements. For example, in a live monitoring situation, where a rapid assessment of the scene or situation may be needed, a higher screen occupation may be required than a system which is required to be more 'reactive', whereby little or no live interaction is anticipated and recordings / events can be reviewed in slower time.

Where there is a need to use images for AFR then image quality should be a key consideration, i.e. the images should be of a quality that is suitable for capturing facial images, i.e. the objective should be to reduce the risk of error, ideally without error.

6.6. Environmental considerations

Consideration should be given to the need for specialist equipment or installation techniques in certain environments.

For example, consideration should be given to the need for intrinsically safe equipment in potentially explosive areas such as petro-chemical environments and corrosion-proof equipment in chemical or marine environments. Equipment should conform to any relevant standards that apply to these environments (e.g. ATEX directive1 for explosive environments).

[1] ATEX 95 equipment directive 94/9/EC, equipment and protective systems intended for use in potentially explosive atmospheres; ATEX 137 workplace directive 99/92/EC, Minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres.

Specific consideration should also be given to installations in areas of extreme heat or extreme cold in order to ensure that these factors have no adverse effect on system operations.

Consideration of environmental requirements should be given to areas which may not be immediately obvious. For example, where hard disk video image storage systems are to be installed which may, in their own right, raise the local temperature to an extent whereby artificial cooling methods such as air conditioning are required to help ensure longevity of the equipment.

6.7. Regulations and legal requirements relevant to VSS

SCCoP Guiding Principles (see ANNEX C)	**Principle 2 states:** The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
	Principle 3 states: There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

There are many legal requirements and regulations that apply to VSS including those listed here. It is the responsibility of the owner, security company (e.g. installer / maintainer) and operator to ensure compliance with these as appropriate to their activities and location. Consideration should also be given to other byelaws introduced by local government. These will vary from region to region.

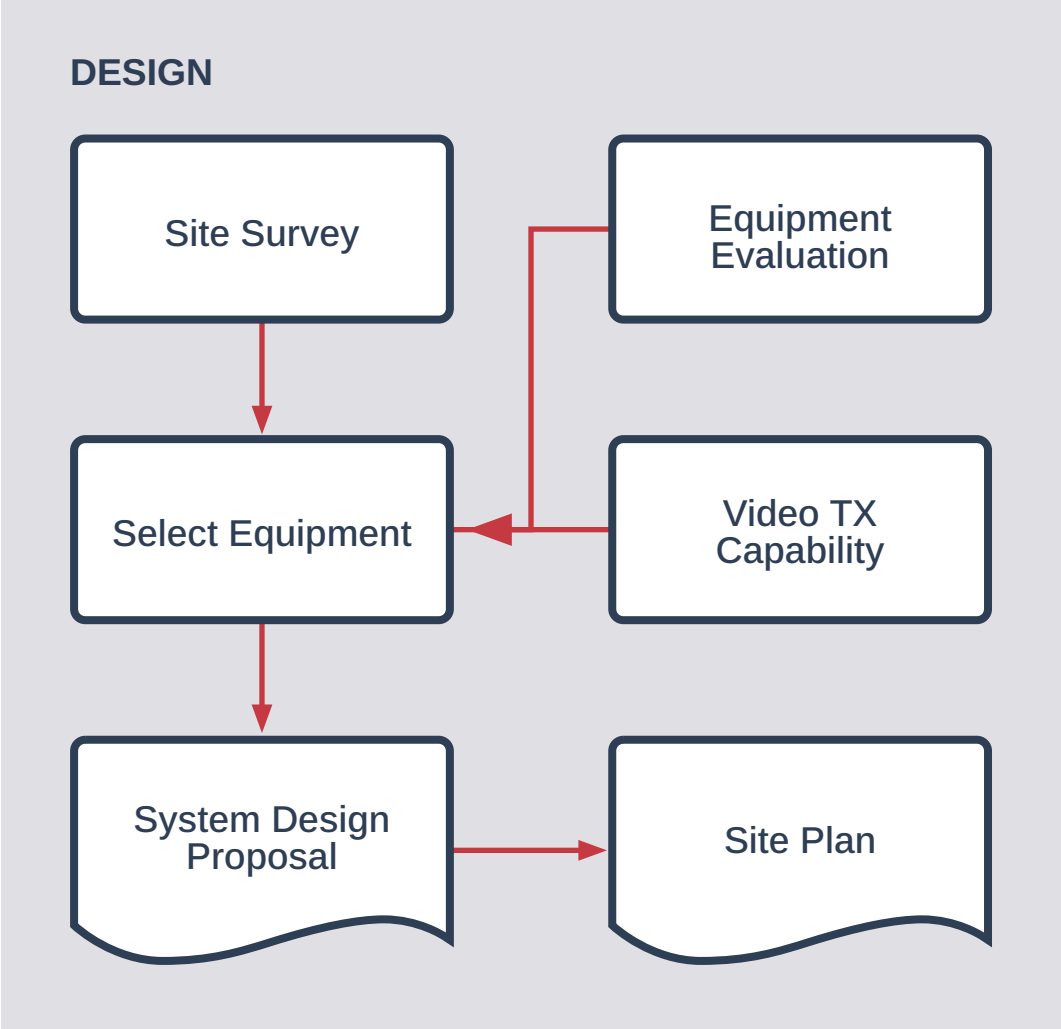
The following Acts of Parliament are known to affect the majority of VSS, but others will apply in specific circumstances:

The Human Rights Act 1998
The Data Protection Act 2018 (DPA).
The Freedom of Information Act 2000
The Private Security Industry Act 2001
The Clean Neighbourhoods and Environment Act 2005
The Protection of Freedoms Act 2012
Road Traffic acts

Further information about these acts and regulations can be found in Annex D

7. Design

7.1. Flowchart



7.2. Site survey

7.2.1. General

A site survey should be conducted to take into account specifics of the site along with the OR. Locations of interest should be established and documented on the site plan.

The level of detail required for the stated performance (e.g. identify) should be established in order to work out the number and type of cameras and the camera positions.

7.2.2. Lighting

The site survey should consider lighting. Depending on circumstances day and night time surveys may be required. The survey should identify areas where lighting may need to be adjusted and/or additional lighting may need to be provided. The selection of cameras and lenses suitable for operation under the proposed light levels should then be carried out.

The performance of a VSS is primarily dependent upon the available light level. It is important, therefore, that the limits of light levels within which an installed system is intended to function are expressed in units of illumination (e.g. lux).

Light levels are normally measured in lux, the SI unit of luminance. In some cases, the amount of light will be quoted in foot-candles. One foot candle is approximately ten lux. Lux levels apply only to visible light spectrum and are not relevant to infrared systems. Table 2 indicates typical lux levels.

Table 2: Typical Lux Levels and Appearance

		Lux level
	*Bright day*	*10,000 to 100,000*
	*Overcast day*	*500 to 10,000*
	*Twilight*	*5 to 500*
	*Night with streetlights*	*1 to 5*
	*Moonlit night (no street lights)*	*0.01 to 1*
	*Dark sky at night*	*0.0001 to 0.01*

7.2.3. Other considerations

The survey should be used to decide the positioning of all key equipment of the system along with the necessary environmental protection requirements.

The site survey should consider power and device interconnection together with provision of local power supplies, routing of cables, wireless links, etc.

During the survey consideration should be given to how the equipment will be installed and other considerations such as accessibility, access times, need for closures whilst equipment is being installed and accessibility for maintenance.

7.2.4. Cybersecurity considerations (where applicable)

Where all or part of the VSS relies on an IP network or the internet to function effectively then some consideration should be given to cybersecurity and ongoing support. For example, how are security updates going be notified and applied to the VSS over its lifecycle to ensure that the system remains cyber secure.

Where the VSS relies upon a third party IP network to function correctly (for example the customer's existing IP network, or an IP network under the control of the customer or customer's sub-contractor) then the customer should be responsible to ensure the cybersecurity of that network. These activities could be ongoing over the lifecycle of the system(s) and may be critical to its successful operation and should therefore be addressed formally, for example, within the system design proposal and as fitted records.

7.3. Equipment selection

7.3.1. General

During system design and equipment selection, consideration should be given to the specification of individual components and the compatibility and performance of components used in conjunction with one another.

Consideration should include environmental factors (e.g. efficient use of power, disposal of consumable items, and control of hazardous substances).

Equipment selection should be matched to achieve OR needs (i.e. monitor, detect, observe, recognise, identify, inspect). Refer to 6.5.

7.3.2. Camera and lens

7.3.2.1. General

A camera and lens should be compatible and should be selected to cover the area to be viewed, considering any person or object required to be identified.
The types of camera selected should be suitable for the application(s).

7.3.2.2. Light sensitivity

There are many different types of camera available with suitability for different applications. A camera that produces good results during daylight hours may not perform well after dusk and a camera suitable for low light level conditions may not work with infrared lighting.

Available light level will have a major influence on the choice of camera and typically the sensitivity of a camera measured under laboratory conditions may not match results under natural operating environments. There may be a trade-off between higher resolution cameras and a reduction in sensitivities.

Colour cameras respond in a similar manner to the human eye but require significantly higher light levels to provide full video signal compared with monochrome cameras. Monochrome cameras and day/night cameras with removable IR cut filters have varying degrees of red and infrared response depending on the imaging device used.

When selecting a camera for a particular application, consideration should be given to the type of light source and the spectral response of the imaging device in addition to the scene reflectance and lens.

Wide dynamic range cameras can help compensate for large variations of luminance across a scene and provide acceptable exposures simultaneously in the brightest and darkest areas of the image. Dynamic range describes the ability to obtain suitable detail from images with mixed light levels. The human eye is capable of discerning detail in a wide range of lighting conditions and a properly adjusted camera can work equally well in each condition but not necessarily all conditions without adjustment.

For example, part of a scene may have a lux level averaging 100 whilst another has a lux level approaching 10,000. If the camera is adjusted to achieve optimal results at 20 to 200 lux then the areas at 10,000 lux will appear washed out with no detail. Image sensing technology that has a wide dynamic range may be used so that a single image can have detail in both the very light and very dark areas. This could also be achieved by utilising suitable software processing.

Selection of the correct lens type is as important as the camera selection. A poor lens performance can significantly detract from the overall performance of the system. For further information refer to BS EN 62676-4 clause 6.5.

For some applications, a thermal imaging camera that responds to heat radiated from a target, rather than reflected light may be appropriate.

7.3.2.3. Field of view

The equipment selection should ensure the field of view will fulfil the operational requirements.

Note: Refer to BS EN 62676-4 clauses 6.7 & 6.8, Home Office guidelines, BSIA Privacy and Chip & PIN guides.

7.3.2.4. Illumination

Depending on the choice of camera equipment and the system's operational requirements extra illumination may be required.

Note: Refer to BS EN 62676-4 clause 6.9 for points to consider e.g. positioning, beam pattern, maintenance, deterioration of light source with age, unwanted reflections, type of lighting and switching.

7.3.2.5. Housings and mountings

All equipment installed should be suitable to withstand the prevailing environmental conditions according to the environmental classes in BS EN 62676-1-1. This includes protection against dust, particles, water and any special environmental conditions that may prevail on the site (e.g. corrosive or explosive atmospheres).

A camera and its supporting hardware should be securely mounted. The camera mounting bracket or pole should safely support the weight and windage of the camera and of any associated hardware. Remember that a small amount of deflection in a pole when a camera is fully zoomed in at a distant target will result in large degrees of movement in the scene.

Consideration should be given to the environmental conditions in which the equipment is intended to operate with respect to the additional features which may be implemented into housings i.e. heaters, wipers.

Protection against malicious damage either through forceful impact, scratching or burning plastic windows or dome bubbles, or spraying should be addressed by using a combination of housing specification and physical positioning.

7.3.2.6. PTZ (Pan-Tilt-Zoom)

Note: BS 8418 uses the term "functional camera" to include cameras using PTZ mounts.

Mechanisms should be specified to take account of the following:

- The maximum required pan and tilt rotation angles and any intermediate preset stops within these.
- Blind spots can be created where PTZ units do not provide full 360 degree rotation. Where this is important for full coverage, a continual rotation PTZ unit should be considered.
- The required rotational speed to meet requirements for tracking objects or to arrive at a preset shot.
- The maximum supported load.

With dome cameras the optical correctness of the dome should be considered especially on long distance views where the lens is positioned close to the edge of the dome bubble. Smoked or mirrored dome covers will reduce the amount of light reaching the camera.

Consideration should be given to cleaning, especially if wash / wipe features are not available.

Note: Refer to BS EN 62676-4 clause 6.4.2

7.3.3. Powering

Consideration should be given to the power requirements of the system.

This includes:

- Local or centrally powered.
- Mains or low voltage.
- Back up / Stand-by power in the event of mains failure.

For Power over Ethernet (PoE) consider the potential need for high power PoE supplies for certain cameras, especially ones with in-built illuminators, heaters or motorised PTZ functions.

For PoE also consider the limiting distance factor of 90m in order to deliver the maximum power from the power sourcing equipment (PoE injector) to the powered device. Greater distances will adversely affect performance of the cabling including bandwidth.

7.3.4. Video performance

Equipment and system design should consider the need to achieve performance levels and characteristics as stated in the operational requirements. This should include consideration of frame rate, resolution and quality of live and recorded images both for human viewing and for automated video analytics.

Degradation of analytic system performance due to resolution and quality reductions over transmission links may be avoided by moving the analytics to the edge device (e.g. camera or encoder).

Performance may be affected by the video transmission capability (see 7.5).

7.3.5. Video image storage characteristics

The total storage requirement for a video image storage or recording device should be estimated before a system is installed, so that hard drives of the appropriate capacity can be specified. It is vital to ensure that sufficient capacity is available to meet the OR and that unnecessary compromises do not have to be made on either the image quality or retention time.

The video image storage requirement will depend on factors such as whether just video, or video and audio are being stored, frame size, required number of frames per second, number of cameras, bit rate of video and audio streams, retention period, requirements for storage resilience (e.g. mirroring or RAID storage), and operating system overhead.

Refer to BS EN 62676-4 clause 10.

Where organisations or businesses are likely to be required to disclose data, there should be some consideration of an appropriate format of the data to be disclosed, this means that the capability of the device or prospective VSS to export data securely to third parties should also be considered.

7.3.6. Image presentation

The image presentation device(s) should be selected after taking account of the nature of the image viewing task, the conditions in the control room or other viewing space and the need to identify, recognise, detect or monitor (see 6.5). It should be considered whether display equipment is also used for viewing maps, floor plans, device lists, system status, alarm conditions, etc.

Display screens have different resolution depending on set-up and type. Display resolution should be selected to match and complement the camera resolution and resultant video resolution.

For larger display surfaces, the efficient display resolution can be defined according to the minimum visible size of a pixel. The size and resolution of display screens should be considered together with the recommended display sizes. An operator placed at a large distance may not be able to discern the details of a small high-resolution monitor. Refer to 62676-4 clauses 7 and 12.

When displaying images where a significant amount of movement is present (e.g. traffic) display refresh rates and resolutions should be matched to the image source.

7.4. System design proposal including site plan

Once the site survey and OR is completed the VSS can be designed and a System Design Proposal (SDP) prepared.

Where an OR is not available, as may be the case for less complex systems, the SDP, drawn up as part of the process of ascertaining the customer's needs, expectations, and patterns of usage of the premises, forms the basis of the agreement between the installing security company and the customer as regards the VSS to be supplied. At appropriate stages checks should be made to ensure that the proposed implementation will meet the customer's operational requirements. The operational requirement and matching test procedure are essential to assess whether the system will fulfil its required purpose.

The SDP for a VSS should draw the customer's attention to:

i. The Data Protection Act (except in clear cases where the DPA does not apply) and the Information Commissioner's Office publication 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

   Note: See Information Commissioners Office website for more information (ico.org.uk).

ii. The requirement to provide signs under the Data Protection Act (except where the DPA does not apply).

iii. British Standard Code of Practice BS 7958 for the management and operation of CCTV (which is applicable to VSS used in public spaces and also provides good practice for all other VSS) and indicate where the document can be obtained.

iv. British Standard Code of Practice BS 8418 for installation of detection activated VSS.

v. British Standards BS 5979 / BS 8591 / BS 9518 / BS EN 50518 for alarm receiving centres and alarm handling (which is applicable to VSS monitoring requiring police response and/or where a defined quality standard for building construction, facilities and operation or an alarm receiving centre are required).

The design should take into account the various requirements and location factors identified in the previous stages. At this stage, a site plan should be drawn up, including locations for the various key components e.g. cameras (including field of view), and PTZ preset positions, detectors (including range and coverage), control rooms, power supplies, interconnections, etc.

The system design proposal should stipulate the conditions under which any test image(s) should be used. For example if the system will be used in both day and night conditions then separate tests should be performed for the different light conditions.

The site plan may be drawn using software (e.g. Computer Aided Design) or hand drawn with annotated pictures taken by a digital camera as appropriate.

Where a system is monitored remotely, a copy of the site plan should be provided to the RVRC / ARC for reference by operators, and the plan should be produced in an acceptable format and quality for that purpose.

Any change to site plans, installation plans, system designs and/or logical architecture should be included and attached to the final documentation and it should include change permissions and risk/ issue/logs generated during the installation process.

Further information can be found in BS EN 62676-4 and BS 8418.

7.5. Video transmission capability (including wireless)

Video transmission capability describes the transfer of video from a capture device (camera) to a viewing device (or software), a recording device (or software) or to a video image storage device using switched networks. The networks may be hard wired or may be wireless. Networks may combine different methods of transmission, e.g. typically described as analogue or IP.

In the case of both wired and wireless networks, sufficient defences should be put in place in order to protect the end user to ensure that the video transmission system is not vulnerable to attack from outside potentially rendering the asset unprotected, or used as a means of penetrating another network to obtain otherwise confidential information.

Where VSS:

- make use of wireless communication links (e.g. transmitting images between devices), this communication should be encrypted to prevent interception.
- transmit images over the internet (e.g. to allow viewing from a remote location or device), this communication should be encrypted to prevent interception and also require some form of authentication for access (e.g. a username and secure password).

The BS EN standards BS EN 62676-2-X comprising part 1, 2 and 3, provide detailed guidelines to manufacturers as to how they should implement IP video transmission products.

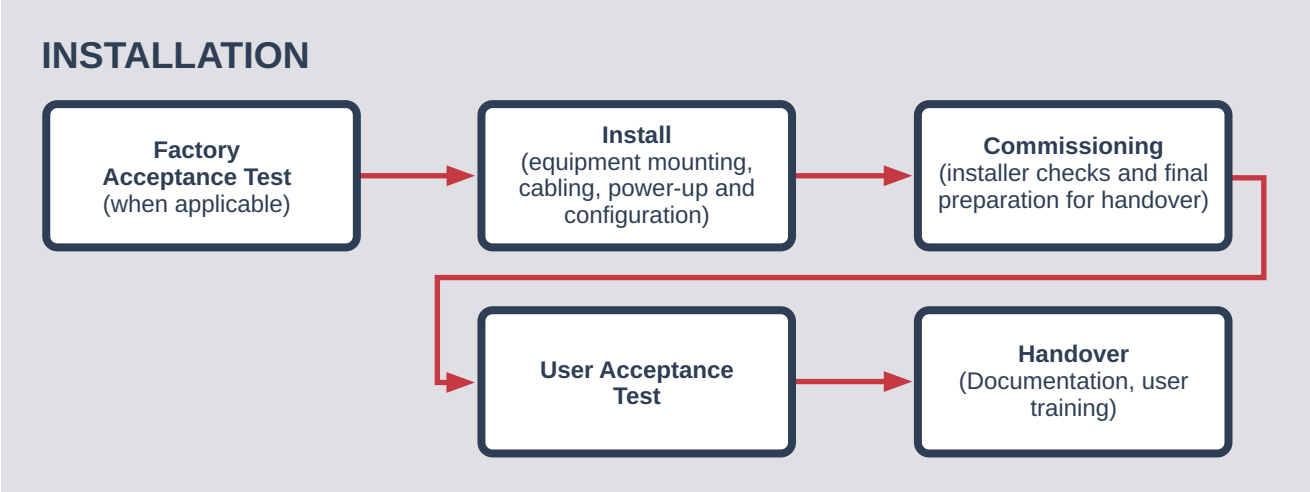
An end user is unlikely to benefit by reading the 62676-2-X standards. They may instead be involved in a buying decision which could place reliance on claims of conformance to the part of the BS EN standard the manufacturer chose to implement. Interoperability of equipment is not solely reliant on the requirements included in the BS EN standards in their current form. There is no guarantee that a product which simply claims BS EN 62676 compliance will provide full compatibility with another claiming the same compliance although it should allow for a minimum level of image transfer. Installers, users and specifiers should treat claims of interoperability between manufacturers products with caution. The parts of the BS EN standard which focus on interoperability, are 62676-2-2, which describes the PSIA guidelines for interoperability of IP Video devices, and 62676-2-3, which describes the ONVIF guidelines for interoperability.

PSIA and ONVIF are at their base level, a common set of commands allowing basic communication between devices, but this does not guarantee that the devices will function to the full potential of their design. Issues with product firmware and software should also be considered: a change of firmware / software versions should be tested separately to ensure continued interoperability. Whilst the specifications try to take this into account, the number of products claiming to be conformant currently makes this an impossible task.

Claims by product manufacturers that PSIA or ONVIF compliance means that users do not have to check that the products work together should be treated with great caution. It is strongly recommended that all such products are tested before being deployed.

8. Installation

8.1. Flowchart



8.2. Equipment evaluation (When is a FAT needed)

Equipment may be required to exchange information in order to perform a function of some kind (for example, to move a PTZ camera to a position based on an input from another system, or increase the record rate and resolution of a device based on the inputs from another device). In these cases, it is recommended the successful operation of the devices be tested first before being deployed. This is particularly recommended if the equipment is made by different manufacturers. This is recommended even when the equipment claims to be interoperable (see notes in 7.5).

Where a customization of a product/software is undertaken in order to meet specific user needs, the customization should be tested with interoperating equipment before being deployed. The customization should also be tested against the user needs defined in the OR.

Refer to BS EN 62676-4 clause 15.1.

8.3. Equipment mounting, cabling, power-up, configuration

8.3.1. Power supplies

Power supplies should be capable of meeting the largest load likely to be placed upon them under normal operating conditions. The maximum load on the power supply typically occurs during start-up of the system following a power failure. The assessment of the electrical current demands for design purposes should also include an extra tolerance of 5% to 10% over capacity.

Where safety and security considerations do not require continued operation of the VSS during a mains supply failure, the public mains supply may be the sole supply for the system.

Note: Some VSS running from a 230 V mains supply require that all equipment be connected to the same electrical phase.

Power supplies should be located within a secure environment, in a position safe from tampering, and should be ventilated in accordance with manufacturer's requirements for safe operation.

All equipment housings should be clearly marked with the operating, or supplied, voltage, whichever is higher.

The installation and position of additional power supplies should be considered if voltage drop across cables is likely to reduce the voltage to equipment to an inoperable level. Alternatively, in some cases, it may be possible to reduce the voltage drop in the cables by using cables with less resistance, greater conductor size or by using more cores of a cable for the supply of power.

8.3.2. Cable installation

The requirements of BS 7671 (Requirements for electrical installations, IET Wiring Regulations) should be met using the edition current at the time of installation.

All interconnecting cables should be fixed and supported and installed to conform to good working practices.

Possible fixings and supports include:

- Conduit: when metal is used, suitable bushes or grommets should be fixed to each end to prevent damage to the cable. When conduit is used to carry the cable it should terminate as close as possible to the unit to be connected.
- PVC or metal trunking: where trunking is used to carry the cable it should terminate as close as possible to the unit to be connected.
- Insulated clips
- Cable ties
- Catenary Cables: When overhead catenary wires with loop holders or plastic buckles are used the supporting wire should be securely attached to the building. Self-supporting catenary cables may be used provided they are correctly designed.

All cables should be of a type and size appropriate to the application and should take account of transmission rate, electrical interference and voltage drop.

Any plastic or PVC component used as part of the installation of cables should be suitable for the environment in which it is installed. Externally mounted ties and clips should be made of UV-resistant material.

Environmental conditions such as dampness, excessive heat, risk of corrosion, mechanical or chemical damage, should be considered when determining the degree of protection required for cable runs.

Any cables used underground should be suitable for that purpose and have adequate protection from mechanical damage. Underground cables should provide a high level of resistance to dampness, chemical reactions, corrosion and rodents.

All cables installed should be supported such that they will not be liable to premature collapse in the event of a fire.

For example, PVC cable clips or ties or trunking or conduit should not be used as the only method of support on an exposed surface, however, where cables are within the ceiling (so it is not an exposed surface) PVC cable clips or ties or trunking or conduit may be used, i.e. there is no possibility of premature collapse of the cables as the ceiling would need to have already collapsed before this is an issue. False ceilings are not considered ceilings in this instance, therefore cables above false ceiling should be supported accordingly, i.e. so that they will not be liable to premature collapse in the event of a fire.

8.3.3. Camera equipment

Cameras should be mounted in positions free from obstructions and, wherever possible, not directly viewing bright light sources. The mounting position should allow installation and maintenance to be carried out in a safe manner.

If cameras are to be mounted on towers or brackets the following environmental considerations should be made:

a) Rigidity, taking into account potential wind velocity, equipment types and equipment mounting and fixing positions.
b) Electrical interference and the possibility of damage by lightning (see BS EN 62305).
c) Dust, airborne particles and other potential sources of corrosion or contamination.
d) Condensation inside housings and other equipment due to changing temperatures.

Tower and bracket equipment should be installed according to the manufacturer's instructions and within loading specifications.

Where movement of towers is possible, cables and cameras should be installed with their safety and protection against tampering taken into consideration.

The alignment and mounting of line of sight transmission equipment (e.g. optical and microwave) is often critical and consideration should be given to the method of alignment and to the rigidity of the mounting.

Note: Natural movements, such as those experienced by tall buildings, can seriously affect system performance.

Wired connections should, wherever possible, be concealed. Mechanical protection of flexible cable to movable cameras should be considered where physical damage is a possibility e.g. metal conduit or flexible conduit.

The camera should be installed in such a way that it is difficult for an unauthorised person to change the field of view of the camera. This can be achieved by installing at a suitable location and height, the use of appropriate physical mounting and possibly further by the use of security fixings.

The camera interconnections (e.g. cabling, antennae) should not be accessible or able to be torn off. Depending on the security grade of equipment, automatic methods should be deployed to detect the change of field of view of the camera according to BS EN 62676-1-1, 6.3.2.3.

Consideration should be given to the detection of loss of video signal, camera obscuring or blinding on any connected camera. An audible and/or visual system alarm should be generated to inform system operators that acknowledgement is needed and, if defined in the OR, this alarm should be mapped to an output for connection to an alarm system.

8.3.4. Control and recording equipment

The environmental conditions under which equipment will be expected to operate should be considered and environmental housings affording appropriate protection should be specified.

Equipment should be installed to manufacturers' instructions. To reduce the risk of condensation a heater should be installed within housings that may be subject to changes in temperature.

Note: Equipment exposed to direct sunlight may require appropriate shielding to avoid the possibility of overheating.

Where there exists the possibility of penetration by solid objects, dust or water, housings that afford appropriate environmental protection should be used. This is typically quoted as an IP Rating in accordance with BS EN 60529.

To prevent tampering, lockable enclosures should be considered to house the control and recording equipment.

A method of security, such as username and secure password, to access control functions should be considered to restrict access to authorised operators. For all control and recording equipment the following should be taken into consideration:

- Temperature
- Airflow of equipment (front to back, side to side, bottom to top, etc), ensuring that the layout of equipment does not have these intakes/outlets blocked
- Humidity

- Dust and other air contamination
- Vibration
- Electrical interference
- Rigidity, taking into account high wind velocity.
- Ease of access for maintenance and service
- Convenience of operator use

For VSS that store images (or data), some consideration should be given to the physical security of the video image storage or recording device such as whether it is kept in a locked room. Some systems may allow for recordings to be stored in an encrypted format which will prevent unauthorised access in the event of loss or theft, and which could be considered in addition to a range of appropriate and secure access controls.

8.3.5. Display equipment

The size, resolution and positioning of display equipment should be chosen according to their intended usage, available space and number of operators. Advice is given in Annex E.

Display equipment may be desk or wall mounted with consideration given to the ergonomics of the operator. The display equipment should be installed to minimise the effect of lighting, particularly sunlight, which can adversely affect the viewing experience. Wall or ceiling mounted display equipment should be mounted using suitable brackets in accordance with manufacturer's instructions.

Consideration should be given to the positioning of such screens to ensure they are above head height or not in a position where people may bang their head on them.

8.4. Commissioning, handover and documentation

SCCoP Guiding Principles (see ANNEX C)	**Principle 4 states:** There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

8.4.1. General

Commissioning should consist of the inspection and testing of the installed system by the installation technician; handover requires the demonstration of the system to the user and the subsequent acceptance of the installation by the customer.

8.4.2. Commissioning and testing

Commissioning should include visual and functional testing to ensure that:

a) The system is installed in strict accordance with the agreed specification and that the standard of workmanship is high, and

b) The commissioning requirements of this Code of Practice and BS EN 62676-4 are met.

A system test plan should be agreed, and the tests should be selected to demonstrate during handover that the VSS meets the agreed specifications, including those given in the OR.

This should include testing of the following aspects of the system(s):

- All wiring is correctly terminated.
- Supply voltage is correct to all appropriate parts of system. Where extra low voltage cameras are used, the voltage at each camera should be recorded.
- Operation of all monitoring, switching and recording equipment (including time synchronisation) is satisfactory, including playback equipment.
- Interfaces with alarms (e.g. movement alarms, fences) are satisfactory and triggering of alarms is correct.
- Beam interruption detectors are aligned correctly, where used for triggering the VSS.
- Appropriate notices to indicate that 'video surveillance is in operation' have been provided.

- All indicator lamps are working.
- If a standby power supply is specified, ensuring that the system continues to operate correctly to specification when the mains supply is disconnected.

This should also include testing of the following aspects for each camera:

- Camera type and lens fitted is correct for each position.
- Operation of all automatic and / or remotely controlled camera functions (e.g. pan, tilt, zoom, focus, electronic iris, wiper) is satisfactory.
- Correct setting of all pan and / or tilt limits.
- Camera movement, and field(s) of view seen through the appropriate monitor(s), is correct and free from obstruction.
- Operation of electronic irises and focus is satisfactory under the range of intended light levels (night conditions may be simulated through use of suitable neutral density filters).
- Satisfactory operation of supplementary lighting.
- Warning labels are in place in respect of possible sudden movement of camera positioning equipment and in respect of any devices that could cause injury, including damage to the eye.

More information on test methods is provided in BS EN 62676-4, Annex B or C

These test methods may be used wherever an objective evaluation is required to confirm that the required performance can be obtained. The use of the test methods listed above is a matter for agreement between customer and installer and is not a requirement for every installation. Other test methods are permissible.

An example commissioning checklist is shown in Annex F.

8.4.3. Handover

At handover, the installing security company should:

- Demonstrate all aspects of the system operation to the customer, including any necessary safety precautions.
- Ensure that the correct documentation (see 8.4.4) is given to the customer to enable the system to be operated, adjusted and maintained.
- Train the system user(s) in its correct operation and arrange for any necessary future training.
- Ensure that users know the procedure for summoning assistance in the event of system malfunction.

An example handover checklist is given in Annex G.

Following handover the customer should be asked to sign an acceptance document and to enter any confidential information (e.g. secure passwords which restrict user access to engineer and other reserved functions) required to make the system perform to the agreed specification.

An example acceptance document is given in Annex G.

8.4.4. Documentation

Upon completion of a VSS installation there should be a record for each system making up the installation, which should include the following information where appropriate:

a) The name and address of the protected site.
b) The name and address of the customer.
c) The location of each control unit and the type and location of each camera and its associated hardware.
d) An indication of the camera view(s), their purpose(s), and the area(s) protected should be documented. The camera view(s) may be provided in the form of a drawing, a hard copy printout or a video recording.
e) The type and location of power supplies.
f) Details of those cameras that the customer has the facility to manoeuvre or isolate.
g) The type and location of monitors and indicating and / or warning devices.
h) Manufacturer's documentation relating to equipment and its operational settings/controls.
i) Full instructions for the correct use of system, including details of routine testing procedures and any necessary maintenance requirements (see 9); possible sources of interference with the system and equipment with which the system itself will interfere should be identified.
j) The operation, image storage and cycling of recording media.

The make and model number of all items of equipment should be stated in the system record. The system record (i.e. for the "as installed" system) should be agreed with the customer and a copy provided to the customer.

The customer should be offered drawing(s) of the VSS installation. Where symbols are used in drawings, a key to these symbols should always be provided to enable customers to understand the content of the drawings.

The customer should be provided with the record of the results of the objective test where this was agreed to be a requirement.

All documentation referring to a security system should be kept in a place to which access is restricted to authorised persons.

9. Maintenance

Effective and regular maintenance of a VSS is essential to ensure that the system remains reliable at all times. Regular maintenance by a competent security company, and effective failure reporting by the user, will enable potential problems to be identified at an early stage so that appropriate action can be taken.

A maintenance agreement should be agreed between the competent security company and the user of the VSS and should include the following:

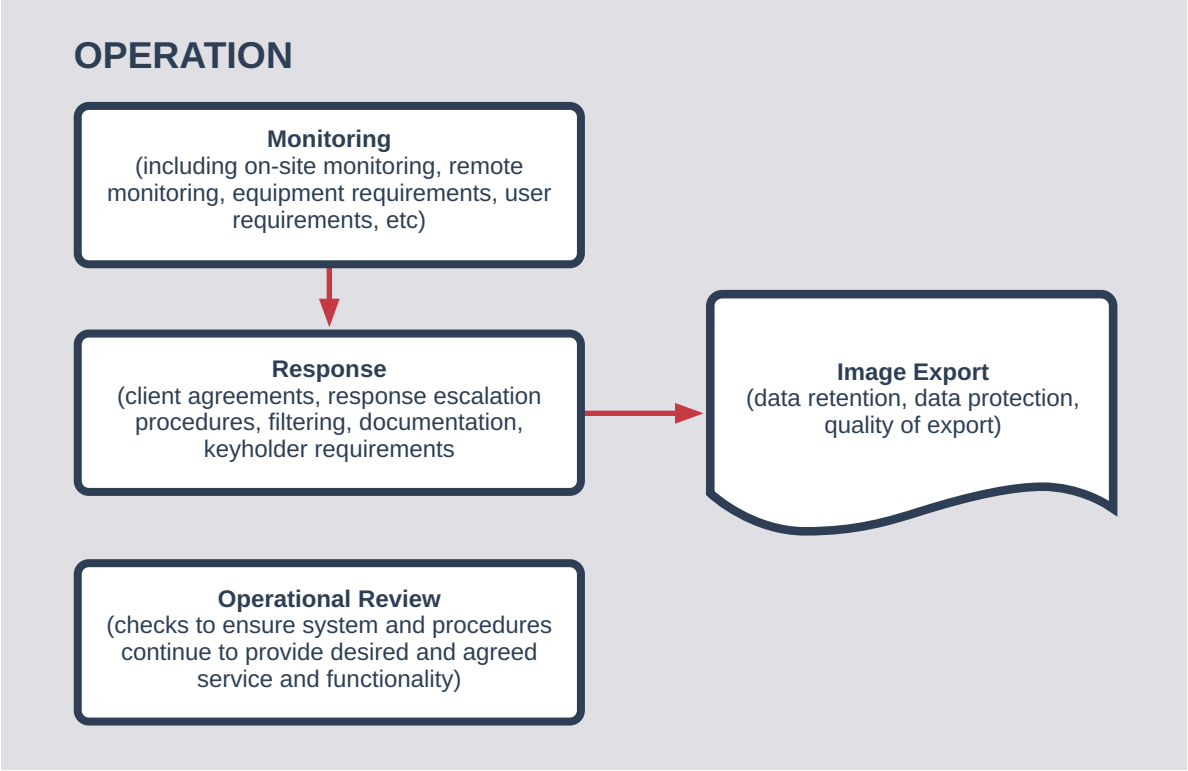
- Preventative maintenance visits - planned servicing of a system, carried out on a scheduled basis confirming that the system(s) continue to function as intended by the system design and fulfil the prevailing OR.
- Corrective maintenance - Emergency servicing of a system, or part thereof, carried out in response to the development of a fault.
- User maintenance - Basic responsibility of the user to maintain operation of the VSS.

Recommendations for maintenance of VSS can be found in BSIA Form 120 - Code of Practice for the maintenance of VSS.

10. Operation

SCCoP Guiding Principles (see ANNEX C)	**Principle 5 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.
	Principle 11 states: When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
	Principle 12 states: Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

10.1. Operation flowchart



10.2. Monitoring

SCCoP Guiding Principles (see ANNEX C)	**Principle 9 states:** Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

Monitoring requirements of a VSS will vary greatly dependant on many factors, such as whether there is a need to view live and / or recoded images, whether the monitoring be done locally and / or remotely, the complexity of the VSS and the type of response required be it a guarding, key-holder or perhaps police response.

10.2.1. Control rooms - general

BS EN 62676-4 clause 12.1 state:

"If the VSS has a requirement for live viewing, camera control, system management, or any other human intensive tasks, a control room should be specified to house these functions. The 'control room' could be a single workstation, or a large operations centre."

Attention should be given to the ambient lighting within the control room and, if the room has windows, how sunlight will affect the operators' ability to monitor the system. This may influence the overall control room layout or require additional window blinds.

The operator should be presented with a manageable number of video feeds (e.g. is the operator able to suitably view 8 cameras and perform the viewing tasks related to all of those camera views, and their anticipated levels of activity?).

The camera view should be presented to the operator at a size sufficient to allow them to undertake the viewing tasks as above either routinely or by manual or automatic switching of views. (e.g. is the operator being presented with views intended for identification tasks, but displayed as part of a quad view, at a lower resolution, reducing the amount of information available to the operator?).

The operator should be positioned so that they are able to view the information on the display equipment correctly (e.g. is the operator using display equipment that is too far away to be able to observe relevant details).

Display equipment that is used for close inspection of video images are commonly called incident or spot displays and positioned on the workstation. They allow for close inspection of images displayed and offer the greatest likelihood of an operator receiving accurate and timely information.

Spot displays should be positioned directly in front of the operator at between approximately 0.5 – 1.5m and of a sufficient size. They should also be placed so that the operator can easily turn their sitting position to face the display equipment.

It can be advantageous to site two, three or four incident displays on a workstation so that the operator can view the video images on primary display equipment and use the adjacent display equipment to show other images or other system details. Dependant on the operational requirement, having multiple operators each with an independently controlled workstation may allow workload to be shared during envisaged busy periods (e.g. during a sporting event where several incidents of interest may be taking place simultaneously).

VSS display equipment can also be positioned off the workstation in a bank or array called a video wall. This can be beneficial as a greater number of images can be presented.

Advice about screen sizes can be found in Annex E.

See also 8.3.5

10.2.2. Control rooms – BS 7958

BS 7958 is the Code of Practice for the Management and Operation of CCTV systems. Its use is intended where data that might be offered as evidence is received, stored, reviewed or analysed. BS 7958 is applicable to video surveillance schemes used in public places and also to the monitoring of traffic regulations.

BS 7958 can also be used to provide guidance on good practice for video surveillance schemes other than those intended for use in public places.

A control room, known as a "CCTV Image Receiving Centre" in BS 7958, should be designed to incorporate facilities as defined within clause 6 of BS 7958: 2015 and summarised below:

- Be within a dedicated building or a room within a building
- Be kept locked, both while in use and if evacuated
- Have separate facilities for refreshment and rest periods, where possible
- Should have the means for direct communication with the control room of law enforcement agencies
- Access to the CCTV Image Receiving Centre should be strictly controlled, including at shift change
- All visitors and contractors entering the CCTV Image Receiving Centre should sign a visitors log
- The CCTV Image Receiving Centre should be designed in accordance with good ergonomic practice, BS EN ISO 11064-1, BS EN ISO 11064-2 and BS EN ISO 11064-3 give relevant information and attention should also be drawn to the Equality Act 2010

10.2.3. Control rooms – BS EN 50518, BS 9518, BS 5979 & BS 8591

BS EN 50518, BS 9518, BS 5979 & BS 8591 are codes of practice for alarm receiving centres receiving signals from safety and security systems (including VSS). Their use is primarily for the remote monitoring of VSS used in security applications where a high degree of resilience of the monitoring operation is specified.

- *Within BS 5979 and BS 8591 there are two categories of remote centre, category I & II. In terms of VSS monitoring, category II (the higher category) is required where a Police response is necessary to meet the requirements of the system design and OR.*
- *Within BS EN 50518 there are also two categories of remote centre, category I & II. In terms of VSS monitoring, category I (the higher category) is required where a Police response is necessary to meet the requirements of the systems design and OR (note that the categories are reversed in BS EN 50518).*
- *BS 9518 covers the alarm handling and response processes.*

Note: For detection activated VSS installed to BS 8418, the requirements within that standard also apply to be eligible for Police response. See 10.2.4 below.

10.2.4. Control rooms – monitoring of BS 8418 systems

For the monitoring of BS 8418 detection activated VSS, the control room should comply with the following requirements:

- The construction of the facilities of the RVRC/ARC should conform to BS 5979 or BS EN 50518. See 10.2.3 above.
- The management and operation of the RVRC/ARC should conform to BS 7958. See 10.2.2 above.

10.3. Training of operators to gain effective use

Trained operators will help contribute to the effective use of the VSS. The OR will assist in determining who requires training and to what level.

Training should be documented and logged and may be delivered either by the security company during handover and/or the organisation operating the system for new operators and refresher training.

BS EN 50518, BS 9518, BS 5979, BS 8591 and BS 7958 have specific requirements for selection and training of personnel. These requirements should be followed where systems are monitored in accordance with the specified standard.

As, and where required by law, public space VSS operators should be licensed by the SIA (Security Industry Authority). In order to obtain a license, individuals must demonstrate that they have been appropriately trained, guidance is available at www.gov.uk/government/organisations/security-industry-authority

10.4. Procedures for data protection and authorisation of access

VSS operated by businesses and organisations who routinely capture images of individuals should adhere to the requirements and principles of the Data Protection Act (DPA).

The DPA not only creates obligations for organisations, but it also gives individuals rights, such as the right to gain access to their details and to claim compensation when they suffer damage. The basic legal requirement is to comply with the DPA itself. Organisations may use alternative methods to meet these requirements, but if they do nothing then they risk breaking the law.

The Information Commissioners Office has produced 'In the picture: A data protection code of practice for surveillance cameras and personal information' that provides guidance on how to ensure that VSS and their operation comply with the DPA.

Note: See Information Commissioners Office website for more information (ico.org.uk).

10.5. Incident response

10.5.1. General

Locally agreed procedures should detail the action to be taken in the event of an incident. These procedures should conform to those laid out in clause 7 of BS 7958, as outlined below:

- Action to be taken
- Who should respond
- The timescale for response
- The times at which observation should take place
- The criteria for a successful response

VSS operators should maintain a record of all incidents in the appropriate incident log.

Note: Attention is drawn to the obligations placed upon investigators by the Criminal Procedure and Investigation Act.

10.5.2. Making the response

The procedures should identify who is responsible for making the response to an incident. Depending on the incident, this should be one of the following:

- The relevant law enforcement agency/authority
- Private security staff
- Store detectives
- Key holders
- Council employees

10.5.3. Timescale of the response

The time at which the incident is notified to the relevant authority should be documented. The policy and procedures should indicate the times at which observation and/or recording is needed and might include the following guidelines:

- Immediately after an incident
- Until arrest/curtailment
- During a whole incident, initiated by an alarm
- Not incident-related, for example, video loss, detector failure etc
- For specific set periods

10.5.4. Result of a successful response to the incident

The overall indicator of successful response to incidents is that the video surveillance scheme fulfils its objectives, e.g.:

- *Restoration of tranquillity*
- *Dispersal or control of the situation*
- *Prevention or minimization of injury and damage*
- *Reduction of crime and disorder, to improve safety and reassure the public*
- *Identification of a suspect*
- *Gathering relevant information to assist in the subsequent apprehension of offenders*
- *Apprehension of a suspect with evidence*
- *Public safety through effective evacuation*
- *Traffic flow restored*

10.6. Recording quality and image storage/retention time

SCCoP Guiding Principles (see ANNEX C)	**Principle 6 states:** No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once its purpose has been discharged.
	Principle 7 states: Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
	Principle 9 states: Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10.6.1. General

Recorded material should be suitable for evidential use as required by the courts if it is to be admitted as evidence; it is therefore essential that recorded material evidence maintains total integrity and continuity at all times.

Modern technology enables data to be recorded and stored on a variety of recording materials; the good practice set out in this code of practice should be applied and modified to suit the specific recording material being used by a VSS. If recorded data is held on an electronic document management system, the system should conform to BS 10008.

Appropriate security measures should be taken to prevent unauthorized access to the system, this will prevent unauthorized or unintentional alteration, disclosure, loss or destruction of recorded material.

Data should not be released to organizations outside the ownership of the video surveillance scheme, other than under guidelines referring to the release of information for the purposes of identifying alleged offenders or witnesses, in accordance with the particular control room's policy and procedure.

A hard copy print should not be made as a matter of routine. If such a print is made the person making it should be responsible for recording the full circumstances under which the print is taken, with reasons, in accordance with procedures. Ideally, each print should be allocated a unique number and recorded in the appropriate log.

10.6.2. Media use, recorded material storage and disposal

Recorded material should be stored in a secure environment, so that the integrity of the media is maintained. This includes recorded material that has been requested by the law enforcement agencies or contains a known incident. Controlled access to the recorded material storage area should be strictly maintained. Data that is to be destroyed should be destroyed under controlled operation.

10.6.3. Recorded material register

The recorded material register should show the life of the media at all stages whilst in the owner's possession; such a register may also show itself to be useful in enabling evaluation of the video surveillance scheme. The register should include the following:

- Unique equipment reference number
- Time/date/person removing equipment from secure storage for use
- Time/date/person returning equipment to secure storage after use
- Remarks column to cover additional points (e.g. erase/destroy/handed over to law enforcement agencies/removed from recording machine)
- Time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned
- In the event of a non-automated system of erasure of data, the time/date/person responsible for erasure and/or destruction

10.7. Databases

SCCoP Guiding Principles (see ANNEX C)	**Principle 12 states:** Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Whenever a VSS is used in conjunction with a database it is essential that the database is maintained, accurate and up to date. The source of any information should be assessed for accuracy before use. The database should comply with all relevant legislation including compliance with the Data Protection Act. A policy should be in place to ensure the information is accurate.

Examples of associated databases are those used for ANPR and AFR.

10.8. Exporting recordings

When exporting recordings, the following procedure should be followed:

- Maintain records of the operator(s) of the equipment. This enables the manager to establish who was operating the equipment at any given time.
- Record without interruption, wherever practicable. Any interruption should be logged.

The export of data should conform to the 'Digital imaging procedure and UK police requirements for digital CCTV Systems'.

Further guidance can be found in HOSDB publications:

PSDB 09/05	HOSDB/ACPO UK Police Requirements for Digital CCTV Systems
HO 66/08	HOSDB - Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0
HO 58/07	HOSDB Digital Imaging Procedure

The documents referenced above can be found at:
https://www.gov.uk/government/publications/cctv-guidance

Note: Computer programs may be used for this purpose provided nobody can tamper with, or edit, them after the event. If records are maintained on an electronic document management system, the system should conform to BS 10008.

10.9. Review of operational needs

SCCoP Guiding Principles (see ANNEX C)	**Principle 10 states:** There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

The system owner should conduct a review at regular intervals not exceeding 12 months to:

- Ensure any changes in the operational requirements of the VSS are identified.
- Identify any system improvements that could enhance the system's ability to fulfil the operational requirements.

It is recommended that the security company providing design input and/or maintenance of the system are involved in any review and that any identified changes are recorded, together with an agreement detailing any work to be carried out.

Examples of things to be considered during the review include:

- *Changes to use of the property*
- *Changes in the adjacent area (e.g. affecting sunlight, shadows, likelihood of pedestrian or vehicle movement)*
- *Growth of vegetation (blocking views, casting shadows, encouraging animals, providing shielding for intruders, etc)*
- *Changes in the threats*
- *Changes in monitoring ability (e.g. staff resource)*
- *Improvement in detector, camera and recording technology*
- *Changes in legislation*

Where changes are identified that may remove the need for video surveillance it is recommended that the need to continue surveillance is considered in respect of regulations (e.g. Protection of Freedoms Act, Human Rights Act, etc).

Note: The review of the operational requirements may be based on attempts to measure the effectiveness of the system. Care should be taken when reviewing system operational needs on the basis of such measurements. For example, in response to a number of crimes in year 1 a VSS is fitted and in year 2 a number of criminals are caught. In year 3 no criminals are caught. This does not imply that the cameras are no longer effective because the crime may have been displaced because of the effectiveness of the cameras.

Annex A – The condensed code

Clause	Item	Content	Reference / comment
6.2		**Capturing user need**	**SCCoP Guiding Principle 1** BS EN 62676-4 Clause 4.2.
6.2	1	It is the responsibility of the system specifier or purchaser to identify and record the purpose of the VSS	
6.2	2	Ensure the fundamental reasons for the system are recorded in the Operational Requirement (OR) or System Design Proposal (SDP).To enable effective planning of an installation and to ensure that the design outcomes yield a suitable solution, the security company should capture as much pertinent information as possible from the client.	BS EN 62676-4 Clause 5.2
6.3		**Threat, vulnerability, risk assessment**	BS EN 62676-4 Clause 4.2.
6.3	1	A threat, vulnerability and risk assessment should be performed.	
6.3	2	The result of the threat, vulnerability and risk assessment should be recorded as part of an OR or SDP. In some cases the system owner may prefer to restrict access to the full assessment and provide only the conclusions to the security company. This should be recorded.	
6.4		**Establishing operational requirements and agreeing with customer**	BS EN 62676-4 Clause 4.3 BS EN 62676-4 Clause 5
6.4	1	Operational requirements should be documented to clearly define the needs and expectations of the VSS and its relevance to the threat, vulnerability and risk assessment.	
6.4	2	The OR (or SDP) should include the following information: • Definitions of areas under surveillance • Limitations of surveillance – This may include any local legislations or privacy issues • Activity to be captured – Definition of targets – Observation category of target (e.g. detect, recognise, identify – see 6.5) • Image / picture performance – e.g. level of detail operator to be able to perceive • Periods of anticipated operation / usage • Site Conditions – Specific issues which may affect camera views such as fog, large vehicle movement, lighting conditions • Resilience – i.e. need for backup power supplies, cybersecurity etc. • Video image storage and monitoring requirements – Image recording rates for normal and event periods – Retention period (how long images should be stored for) – Where and who should be able to monitor images • Extracting / Exporting images – Procedures – Who and where can be carried out – Media to be extracted to – Likely periods / quantity of data to be exported • Operational response – Persons responsible for responding – Response procedures – Response times	

Clause	Item	Content	Reference / comment
		• Training – Definition of training required for different elements of the system, e.g. routine monitoring, image export etc. – Quantities of persons requiring training • Planned or possible future expansions to the system, including addition of further cameras, monitoring locations and integration to other systems	
6.5		**Target capture and image detail**	BS EN 62676-4 Clause 6.7 BS EN IEC 62676-5
6.5	1	The level of detail required in an image should be discussed with the client and recorded (i.e. monitor, detect, observe, recognise, identify, inspect)	
6.6		**Environmental Considerations**	BS EN 62676-4 Clause 5.3.7 BS EN 62676-4 Clause 6.4.1 BS EN 62676-4 Clause 6.5 BS EN 62676-4 Clause 12.9
6.6	1	Consider the need for specialist equipment or installation techniques in certain environments.	
6.6	3	Consideration of environmental requirements should be given to areas which may not be immediately obvious.	
6.7		**Regulations and legal requirements relevant to VSS**	**SCCoP Guiding Principle 2 & 3** BS EN 62676-4 Clause 16.5
6.7	1	It is the responsibility of the owner, security company (installer / maintenance), and operator to ensure compliance with legal requirements and regulations as appropriate to their activities and location. This includes local byelaws.	
7		**Design**	
7.2		**Site survey**	BS EN 62676-4 Clause 4.4 BS EN 62676-4 Clause 4.5
7.2.1	1	Conduct a site survey to take into account specifics of the site along with the OR.	
7.2.1	2	Establish locations of interest and document on a site plan	
7.2.1	3	Establish level of detail required for the stated performance (e.g. identify) to work out the number and type of camera and the camera positions.	
7.2.2		**Lighting**	BS EN 62676-4 Clause 6.9
7.2.2	1	Consider lighting. Depending on circumstances day and nighttime surveys may be required.	
7.2.2	2	Identify areas where lighting may need to be adjusted and/or additional lighting may need to be provided.	
7.2.2	3	Select cameras and lenses suitable for operation under the proposed light levels.	
7.2.3		**Other considerations**	
7.2.3	1	Use the survey to decide the positioning of all key equipment of the system along with the necessary environmental protection requirements	BS EN 62676-4 Clauses 6.5, 6.11.1 and 6.11.2
7.2.3	2	The site survey should consider power and device interconnection together with provision of local power supplies, routing of cables, wireless links, etc.	
7.2.3	3	During the survey give consideration to how the equipment will be installed and other considerations such as accessibility, access times, the need for closures whilst equipment is being installed and accessibility for maintenance.	

Clause	Item	Content	Reference / comment
7.2.4		**Cybersecurity considerations**	
7.2.4	1	Where all or part of the system relies on an IP network or the internet to function effectively then some consideration should be given to cybersecurity and ongoing support.	
7.2.4	2	Where the VSS relies upon a third-party IP network to function correctly (for example the customer's existing IP network, or an IP network under the control of the customer, or customer's sub-contractor) then the customer should be responsible to ensure the cybersecurity of that network.	
7.3		**Equipment selection**	BS EN 62676-4 Clause 6
7.3	1	During system design and equipment selection give consideration to the specification of individual components and the compatibility and performance of components used in conjunction with one another.	
7.3	2	Consider environmental factors (e.g. efficient use of power, disposal of consumable items, and control of hazardous substances).	
7.3	3	Equipment selection should be matched to achieve OR needs (i.e. monitor, detect, observe, recognise, identify, inspect).	Refer to 6.5
7.3.2		**Camera and lens**	
7.3.2.1	1	Cameras and lenses should be compatible and should be selected to cover the area to be viewed, taking into account any person or object required to be identified.	BS EN 62676-4 Clauses 6.2 to 6.5
7.3.2.1	2	Ensure the types of camera selected are suitable for the application(s).	BS EN 62676-4 Clauses 6.2 to 6.4
7.3.2.2	3	When selecting a camera for a particular application, give consideration to the type of light source and the spectral response of the imaging device in addition to the scene reflectance and lens.	BS EN 62676-4 Clause 6.2 to 6.4
7.3.2.3	1	Ensure the field of view will meet the OR.	BS EN 62676-4 Clause 6.8
7.3.2.4	1	Determine whether extra illumination is required.	BS EN 62676-4 Clause 6.9
7.3.2.5	1	All equipment installed should be suitable to withstand the prevailing environmental conditions according to the environmental classes in BS EN 62676-1-1. This includes protection against dust, particles, water and any special environmental conditions that may prevail on the site (e.g. corrosive or explosive atmospheres).	BS EN 62676-4 Clause 6.5
7.3.2.5	2	Mount cameras and supporting hardware securely.	BS EN 62676-4 Clause 6.5
7.3.2.5	3	Ensure the camera mounting bracket or pole safely supports the weight and windage of the camera and of any associated hardware.	BS EN 62676-4 Clause 6.5
7.3.2.5	4	Give consideration to the environmental conditions in which the equipment is intended to operate with respect to the additional features which may be implemented into housings i.e. heaters, wipers.	BS EN 62676-4 Clause 6.5
7.3.2.5	5	Protection against malicious damage either through forceful impact, scratching or burning plastic windows or dome bubbles, or	BS EN 62676-4 Clauses 6.11.1 and 6.11.2
		spraying should be addressed by using a combination of housing specification and physical positioning.	BS EN 62676-4 clause 6.4.2
7.3.2.6	1	PTZ mechanisms should be specified to take account of the following: • The maximum required pan and tilt rotation angles and any intermediate preset stops within these. • Blind spots can be created where PTZ units do not provide full 360-degree rotation. Where this is important for full	BS EN 62676-4 clause 6.4.2

Clause	Item	Content	Reference / comment
		• Blind spots can be created where PTZ units do not provide full 360-degree rotation. Where this is important for full coverage, a continual rotation PTZ unit should be considered. • The required rotational speed to meet requirements for tracking objects or to arrive at a preset shot. • The maximum supported load.	
7.3.2.6	2	Give consideration to cleaning, especially if wash / wipe features are not available.	
7.3.3		**Powering**	
7.3.3	1	Consideration should be given to the power requirements of the system including: • Local or centrally powered • Mains or low voltage • Back up / Stand-by power in the event of mains failure.	BS EN 62676-4 Clauses 6.1, 12.8
7.3.4		**Video performance**	BS EN 62676-4 Clause 9
7.3.4	2	Equipment and system design should take into account the need to achieve performance levels and characteristics as stated in the OR.	
7.3.4	2 3	Give consideration to frame rate, resolution and quality of live and recorded images both for human viewing and for automated video analytics.	
7.3.5		**Video image storage characteristics**	
7.3.5	1	Estimate the total video image storage requirement for digital video image storage or recording device before system installation and specify a hard drive of the appropriate capacity to meet the OR.	Refer to BS EN 62676-4 clause 10
7.3.6		**Image presentation**	
7.3.6	1	The image presentation device(s) should be selected taking account of: • The nature of the image viewing task • The conditions in the control room or other viewing space • The need to identify, recognise, detect or monitor • Whether display equipment is also used for viewing maps, floor plans, device lists, system status, alarm conditions, etc.	BS EN 62676-4 Clause 7.1
7.3.6	2	Select display resolution to match and complement the camera resolution and resultant video resolution.	Refer to 62676-4 clauses 7.2 and 12
7.3.6	3	Select display refresh rates and resolutions matched to the image source.	
7.4		**System design proposal including site plan**	BS EN 62676-4 Clause 4.5 BS EN 62676-4 Clause 5.2 BS EN 62676-4 Clause 6.6 BS EN 62676-4 Clause 13.3.3
7.4	1	During system design check that the proposed implementation will meet the customers' operational requirements.	
7.4	2	A test procedure should be created to match the operational requirements.	
7.4	3	The SDP for a VSS should draw the customer's attention to: (i) The Data Protection Act (except in clear cases where the DPA does not apply) and the Information Commissioner's Office publication 'In the picture: A data protection code of practice for surveillance cameras and personal information'. (ii) The requirement to provide signs under the Data Protection Act (except where the DPA does not apply).	

Clause	Item	Content	Reference / comment
		(iii) British Standard Code of Practice BS 7958 for the management and operation of CCTV (which is applicable to VSS used in public spaces and also provides good practice for all other VSS) and indicate where the document can be obtained. (iv) British Standard Code of Practice BS 8418 for installation of detection activated VSS systems. (v) British Standard BS 5979 / BS 8591 / BS 9518 / BS EN 50518 for alarm receiving centres and alarm handling (which is applicable to VSS monitoring requiring police response and/or where a defined quality standard for building construction, facilities and operation or an alarm receiving centre are required).	
7.4	4	The design should take into account the various requirement and location factors identified in the previous stages. At this stage, a site plan should be drawn up, including locations for the various key components e.g. cameras (including field of view), and PTZ preset positions, detectors (including range and coverage), control rooms, power supplies, interconnections, etc.	
7.4	5	The system design proposal should stipulate the conditions under which any test image(s) should be used. For example if the system will be used in both day and night conditions then separate tests should be performed for the different light conditions.	
7.4	6	Where a system is monitored remotely, a copy of the site plan should be provided to the RVRC / ARC for reference by operators, and the plan should be produced in an acceptable format and quality for that purpose.	
7.4	7	Any change to site plans, installation plans, system designs and/or logical architecture should be included and attached to the final documentation and it should include change permissions and risk/issue/logs generated during the installation process.	Further information can be found in BS EN 62676-4 and BS 8418
7.5		**Video transmission capability**	BS EN 62676-4 Clause 6.10 BS EN 62676-4 Clause 8
7.5	1	In the case of both wired and wireless networks, sufficient defences should be put in place in order to protect the end user to ensure that the video transmission system is not vulnerable to attack from outside potentially rendering the asset unprotected, or used as a means of penetrating another network to obtain otherwise confidential information.	BS EN 62676-2-X comprising part 1, 2 and 3
7.5	2	Where VSS: • make use of wireless communication links, this communication should be encrypted to prevent interception. • transmit images over the internet, this communication should be encrypted to prevent interception and also require some form of authentication for access (e.g. a username and secure password).	
8.2		**Equipment evaluation**	
8.2	1	Where a customization of a product/software is undertaken in order to meet specific user needs, the customization should be tested with interoperating equipment before being deployed. The customization should also be tested against the user needs defined in the OR.	Refer to BS EN standard 62676-4 clause 15.1
8.3.1		**Power supplies**	BS EN 62676-4 Clause 6.1 BS EN 62676-4 Clause 12.8

Clause	Item	Content	Reference / comment
8.3.1	1	Power supplies should be capable of meeting the largest load likely to be placed upon them under normal operating conditions. The maximum load on the power supply typically occurs during start-up of the system following a power failure. The assessment of the current demands for design purposes should also include an extra tolerance of 5% to 10% over capacity.	
8.3.1	2	Where safety and security considerations do not require continued operation of the VSS during a mains supply failure, the public mains supply may be the sole supply for the system.	
8.3.1	3	Power supplies should be located within a secure environment, in a position safe from tampering, and should be ventilated in accordance with manufacturers' requirements for safe operation.	
8.3.1	4	All equipment housings should be clearly marked with the operating, or supplied, voltage, whichever is higher.	
8.3.1	5	The installation and position of additional power supplies should be considered if voltage drop across cables is likely to reduce the voltage to equipment to an inoperable level. Alternatively, in some cases, it may be possible to reduce the voltage drop in the cables by using cables with less resistance, greater conductor size or by using more cores of a cable for the supply of power.	
8.3.2		**Cable installation**	
8.3.2	1	The requirements of BS 7671 (Requirements for electrical installations, IET Wiring Regulations) should be met using the edition current at the time of installation.	BS EN 62676-4 Clause 15.2
8.3.2		All interconnecting cables should be fixed and supported and installed to conform to good working practices.	
8.3.2	3	Possible fixings and supports include: • Conduit: when metal is used suitable bushes or grommets should be fixed to each end to prevent damage to the cable. When conduit is used to carry the cable it should terminate as close as possible to the unit to be connected. • PVC or metal trunking: where trunking is used to carry the cable it should terminate as close as possible to the unit to be connected. • Insulated clips • Cable ties • Catenary Cables: When overhead catenary wires with loop holders or plastic buckles are used the supporting wire should be securely • attached to the building. Self-supporting catenary cables may be used • provided they are correctly designed.	
8.3.2	4	All cables should be of a type and size appropriate to the application and should take account of transmission rate, electrical interference and voltage drop.	
8.3.2	5	Any plastic or PVC component used as part of the installation of cables should be suitable for the environment in which it is installed. Externally mounted ties and clips should be made of UV-resistant material.	
8.3.2	6	Environmental conditions such as dampness, excessive heat, risk of corrosion, mechanical or chemical damage, should be taken into account when determining the degree of protection required for cable runs.	

Clause	Item	Content	Reference / comment
8.3.2	7	Any cables used underground should be suitable for that purpose and have adequate protection from mechanical damage. Underground cables should provide a high level of resistance to dampness, chemical reactions, corrosion and rodents.	
8.3.2	8	All cables installed should be supported such that they will not be liable to premature collapse in the event of a fire. For example, PVC cable clips or ties or trunking or conduit should not be used as the only method of support on an exposed surface, however, where cables are within the ceiling (so it is not an exposed surface) PVC cable clips or ties or trunking or conduit may be used, i.e. there is no possibility of premature collapse of the cables as the ceiling would need to have already collapsed before this is an issue. False ceilings are not considered ceilings in this instance, therefore cables above false ceiling should be supported accordingly, i.e. so that they will not be liable to premature collapse in the event of a fire.	
8.3.3		**Camera equipment**	
8.3.3	1	Cameras should be mounted in positions free from obstructions and, wherever possible, not directly viewing bright light sources. The mounting position should allow installation and maintenance to be carried out in a safe manner.	
8.3.3	2	If cameras are to be mounted on towers or brackets the following environmental considerations should be made: a) Rigidity, taking into account potential wind velocity, equipment type and equipment mounting and fixing positions. b) Electrical interference and the possibility of damage by lightning (see BS EN 62305). c) Dust, airborne particles and other potential sources of corrosion or contamination. d) Condensation inside housings and other equipment due to changing temperatures.	
8.3.3	3	Tower and bracket equipment should be installed according to the manufacturer's instructions and within loading specifications.	
8.3.3	4	Where movement of towers is possible, cables and cameras should be installed with their safety and protection against tampering taken into consideration.	
8.3.3	5	The alignment and mounting of line-of-sight transmission equipment (e.g. optical and microwave) is often critical and consideration should be given to the method of alignment and to the rigidity of the mounting.	
8.3.3	6	Wired connections should, wherever possible, be concealed. Mechanical protection of flexible cable to movable cameras should be considered where physical damage is a possibility e.g. metal conduit or flexible conduit.	
8.3.3	7	The camera should be installed in such a way that it is difficult for an unauthorised person to change the field of view of the camera. This can be achieved by installing at a suitable location and height, the use of appropriate physical mounting and possibly further by the use of security fixings.	BS EN 62676-4 Clause 6.11.1
8.3.3	8	The camera interconnections (e.g. cabling, antennae) should not be accessible or able to be torn off. Depending on the security grade of equipment, automatic methods should be deployed to detect the change of field of view of the camera according to BS EN 62676-1-1, 6.3.2.3.	BS EN 62676-4 Clause 6.11.1

Clause	Item	Content	Reference / comment
8.3.3	9	Consideration should be given to the detection of loss of video signal, camera obscuring or blinding on any connected camera. An audible and/or visual system alarm should be generated to inform system operators that acknowledgement is needed and, if defined in the OR, this alarm should be mapped to an output for connection to an alarm system.	
8.3.4		**Control and Recording Equipment**	BS EN 62676-4 Clause 6.11.2 BS EN 62676-4 Clause 12
8.3.4	1	The environmental conditions under which equipment will be expected to operate should be taken into account and environmental housings affording appropriate protection should be specified.	
8.3.4	2	Equipment should be installed to manufacturers' instructions. To reduce the risk of condensation a heater should be installed within housings that may be subject to changes in temperature.	
8.3.4	3	Housings and enclosures have the appropriate IP rating for the environment in which they are located. This is typically quoted as an IP Rating in accordance with BS EN 60529.	
8.3.4	4	To prevent tampering, lockable enclosures should be considered to house the control and recording equipment. A method of security, such as username and secure password, to access control functions should be considered to restrict access to authorised operators.	
8.3.4	5	For all control and recording equipment the following should be taken into consideration: • Temperature • Airflow of equipment (front to back, side to side, bottom to top, etc.), ensuring that the layout of equipment does not have these intakes/ outlets blocked • Humidity • Dust and other air contamination • Vibration • Electrical interference • Rigidity, taking into account high wind velocity. • Ease of access for maintenance and service • Convenience of operator use	
8.3.4	6	For VSS that store images (or data), some consideration should be given to the physical security of the video image storage device such as whether it is kept in a locked room. Some systems may allow for recordings to be stored in an encrypted format which will prevent unauthorised access in the event of loss or theft, and which could be considered in addition to a range of appropriate and secure access controls.	
8.3.5		**Display equipment**	BS EN 62676-4 Clause 12
8.3.5	1	The size, resolution and positioning of display equipment should be chosen according to their intended usage, available space and number of operators. Advice is given in Annex E.	
8.3.5	2	Display equipment may be desk or wall mounted with consideration given to the ergonomics of the operator. The display equipment should beinstalled to minimise the effect of lighting, particularly sunlight, which can adversely affect the viewing experience. Wall or ceiling mounted display equipment should be mounted using suitable brackets in accordance with manufacturer's instructions.	

Clause	Item	Content	Reference / comment
8.3.5	3	Consideration should be given to the positioning of such screens to ensure they are above head height or not in a position where people may bang their head on them.	
8.4		**Commissioning, handover and documentation**	**SCCoP Guiding Principle 4**
8.41	1	Commissioning should consist of the inspection and testing of the installed system by the installation technician; handover requires the demonstration of the system to the user and the subsequent acceptance of the installation by the customer.	
8.4.2		**Commissioning and test**	BS EN 62676-4 Clause 4.6 BS EN 62676-4 Clause 13
8.4.2	1	Commissioning should include visual and functional testing to ensure that: • The system is installed in strict accordance with the agreed specification and that the standard of workmanship is high, and • The commissioning requirements of this code of practice and BS EN 62676-4 are met.	An example Commissioning Checklist is shown in Annex F.
8.4.2	2	A system test plan should be agreed and the tests should be selected to demonstrate during handover that the VSS meets the agreed specifications, including those given in the OR.	BS EN 62676-4 Clause 4.6
8.4.2	3	This should also include testing of the following aspects for each camera: • Camera type and lens fitted is correct for each position. • Operation of all automatic and / or remotely controlled camera functions (e.g. pan, tilt, zoom, focus, electronic iris, wiper) is satisfactory. • Correct setting of all pan and / or tilt limits. • Camera movement, and field(s) of view seen through the appropriate monitor(s), is correct and free from obstruction. • Operation of electronic irises and focus is satisfactory under the range of intended light levels (night conditions may be simulated through use of suitable neutral density filters). • Satisfactory operation of supplementary lighting. • Warning labels are in place in respect of possible sudden movement of camera positioning equipment and in respect of any devices that could cause damage to the eye.	
8.4.2	4	There are test methods given in BS EN 62676-4, Annex B or C. These test methods may be used wherever an objective evaluation is required to confirm that the required performance can be obtained. The use of the test methods listed above is a matter for agreement between customer and installer and is not a requirement for every installation. Other test methods are permissible.	
8.4.3		**Handover**	BS EN 62676-4 Clause 4.7 BS EN 62676-4 Clause 15.4
8.4.3	1	At handover, the security company should: • Demonstrate all aspects of the system operation to the customer, including any necessary safety precautions. • Ensure that the correct documentation (see 8.4.4) is given to the customer to enable the system to be operated, adjusted and maintained. • Train the system user(s) in its correct operation and arrange for any necessary future training. • Ensure that users know the procedure for summoning assistance in the event of system malfunction.	An example Handover Checklist is given in Annex G.

Clause	Item	Content	Reference / comment
8.4.3	2	Following handover the customer should be asked to sign an acceptance document and to enter any confidential information (e.g. secure passwords which restrict user access to engineer and other reserved functions) required to make the system perform to the agreed specification.	An example Acceptance Document is given in Annex G.
8.4.4		**Documentation**	BS EN 62676-4 Clause 4.8 BS EN 62676-4 Clause 15.3 BS EN 62676-4 Clause 16
8.4.4	1	Upon completion of a VSS installation there should be a record for each system making up the installation, which should include the following information where appropriate: • The name and address of the protected site. • The name and address of the customer. • The location of each control unit and the type and location of each camera and its associated hardware. • An indication of the camera view(s), their purpose(s), and the area(s) protected should be documented. The camera view(s) may be provided in the form of a drawing, a hard copy printout or a video recording. • The type and location of power supplies. • Details of those cameras that the customer has the facility to manoeuvre or isolate. • The type and location of monitors and indicating and / or warning devices. • Manufacturer's documentation relating to equipment and its operational settings/controls. • Full instructions for the correct use of system, including details of routine testing procedures and any necessary maintenance requirements (see 9) • Possible sources of interference with the system and equipment with which the system itself will interfere should be identified. • The operation, image storage and cycling of recording media.	
8.4.4	2	The make and model number of all items of equipment should be stated in the system record. The system record (i.e. for the installed system) should be agreed with the customer and a copy provided to the customer.	
8.4.4	3	The customer should be offered drawing(s) of the VSS installation. Where symbols are used in drawings, a key to these symbols should always be provided to enable customers to understand the content of the drawings.	
8.4.4	4	The customer should be provided with the record of the results of the objective test where this was agreed to be a requirement.	
8.4.4	5	All documentation referring to a security system should be kept in a place to which access is restricted to authorised persons.	
9		**Maintenance**	BS EN 62676-4 Clause 17
9	1	A maintenance agreement should be agreed between the competent security company and the user of the VSS and should include the following: • Preventative maintenance visits - Planned servicing of a system, carried out on a scheduled basis confirming that the system continues to function as intended by the system design and meets the prevailing OR. • Corrective maintenance - Emergency servicing of a system, or part thereof, carried out in response to the development of a fault.	

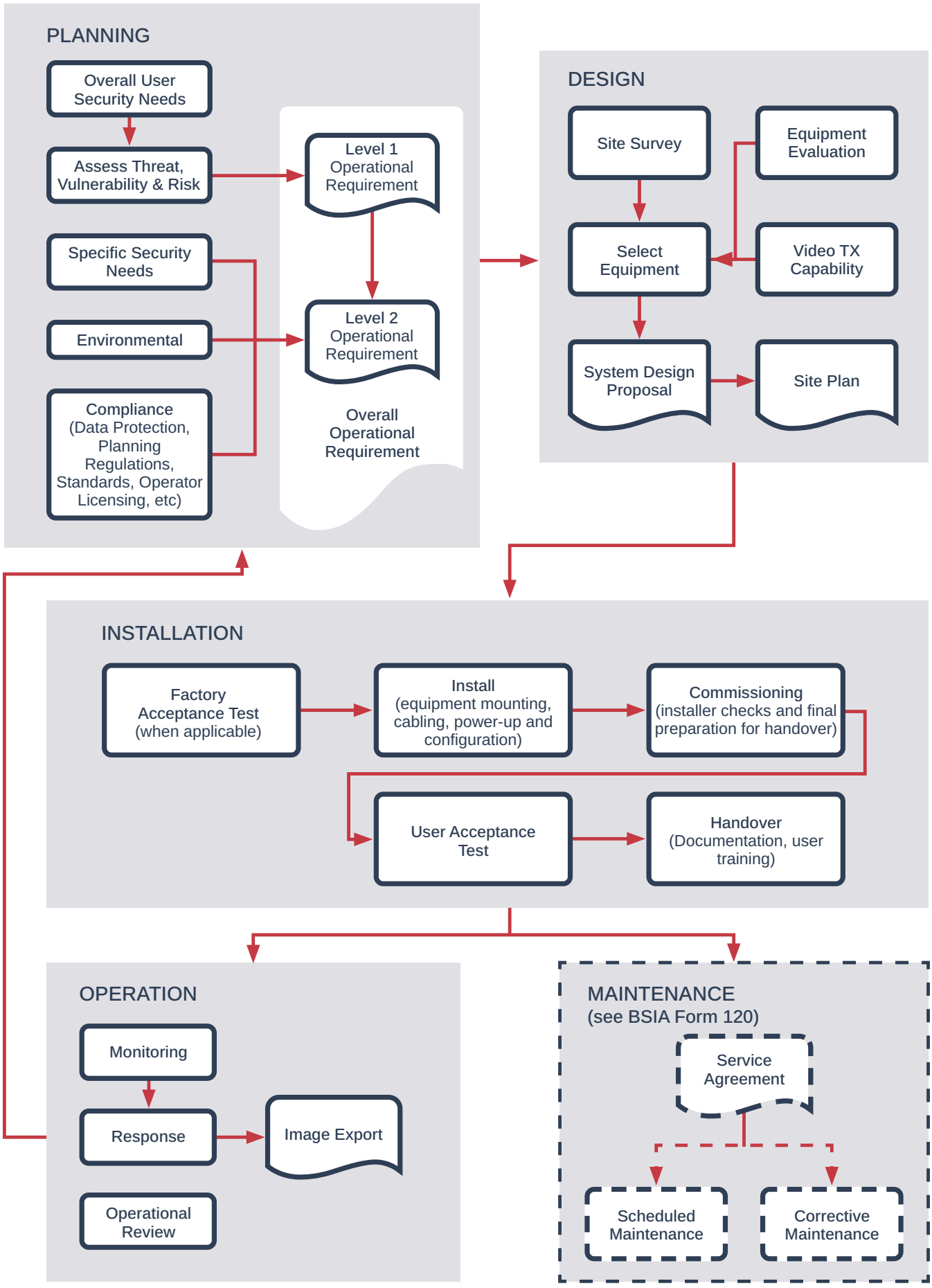
Clause	Item	Content	Reference / comment
		• User maintenance - Basic responsibility of the user to maintain operation of the VSS.	
10		**Operation**	**SCCoP Guiding Principles 5, 11, 12**
10.2		**On-site monitoring**	**SCCoP Guiding Principle 9**
10.2.1		**Control room layout**	BS EN 62676-4 Clause 12
10.2.1	1	Attention should be given to the ambient lighting within the control room and if the room has windows how sunlight will affect the operators' ability to monitor the system.	
10.2.1	2	The operator should be presented with a manageable number of video feeds so they can perform the viewing tasks related to all of those camera views, and the anticipated levels of activity.	
10.2.1	3	The camera view should be presented to the operator at a size sufficient to allow them to undertake the required viewing tasks either routinely or by manual or automatic switching of views.	
10.2.1	4	The operator should be positioned so that they are able to view the information on the display equipment correctly.	
10.2.1	5	Spot displays should be positioned directly in front of the operator at between approximately 0.5 – 1.5m and of a sufficient size. They should also be placed so that the operator can easily turn their sitting position to face the display equipment.	
10.2.2		**Control rooms – BS 7958**	
10.2.2	1	A control room, known as a "CCTV Image Receiving Centre" in BS7958, should be designed to incorporate facilities as defined within clause 6 of BS 7958: 2015 and summarised below: • Be within a dedicated building or a room within a building. • Be kept locked, both while in use and if evacuated. • Have separate facilities for refreshment and rest periods, where possible. • Should have the means for direct communication with the control room of law enforcement agencies. • Access to the CCTV Image Receiving Centre should be strictly controlled, including at shift change. • All visitors and contractors entering the CCTV Image Receiving Centre should sign a visitors' log. • The CCTV Image Receiving Centre should be designed in accordance with good ergonomic practice, BS EN ISO 11064-1, BS EN ISO 11064-2 and BS EN ISO 11064-3 give relevant information and attention should also be drawn to the Equality Act 2010.	
10.2.3		**Control rooms – BS EN 50518, BS 9518, BS 5979 & BS 8591**	
10.2.3	1	BS EN 50518, BS 9518, BS 5979 & BS 8591 are codes of practice for alarm receiving centres receiving signals from safety and security systems (including VSS). Their use is primarily for the remote monitoring of VSS used in security applications where a high degree of resilience of the monitoring operation is specified.	
10.2.4		**Control rooms – monitoring of BS 8418 systems**	
10.2.4	1	For the monitoring of BS 8418 detection activated VSS, the control room should comply with the following requirements: • The construction of the facilities of the RVRC/ARC should conform to BS 5979 or BS EN 50518. See 10.2.3 above. • The management and operation of the RVRC/ARC should conform to BS 7958. See 10.2.2 above.	

Clause	Item	Content	Reference / comment
10.3		**Training of operators**	
10.3	1	Training of operators should be documented and logged.	
10.3	2	Requirements for selection and training of personnel given in BS EN 50518, BS 9518, BS 5979, BS 8591 and BS 7958 should be followed when systems are monitored in accordance with the specified standard.	
10.4		**Data Protection – Access Authorisation**	
10.4	1	VSS operated by businesses and organisations who routinely capture images of individuals should adhere to the requirements and principles of the Data Protection Act.	
10.5		**Incident response**	
10.5.1	1	Locally agreed procedures should detail the action to be taken in the event of an incident. These procedures should conform to those laid out in clause 7 of BS 7958, as outlined below: • Action to be taken. • Who should respond. • The timescale for response. • The times at which observation should take place. • The criteria for a successful response.	
10.5.1	1	VSS operators should maintain a record of all incidents in the appropriate incident log.	
10.5.2	1	The procedures should identify who is responsible for making the response to an incident. Depending on the incident, this should be one of the following: • The relevant law enforcement agency authority. • Private security staff. • Store detectives. • Key holders. • Council employees.	BS EN 62676-4 Clause 5.3.12
10.5.3	1	The time at which the incident is notified to the relevant authority should be documented.	
10.5.3	2	The policy and procedures should indicate the times at which observation and/or recording is needed and might include the following guidelines: • Immediately after an incident. • Until arrest/curtailment. • During a whole incident, initiated by an alarm. • Not incident-related, for example. • For specific set periods.	
10.6		**Recording quality and image storage / retention time**	**SCCoP Guiding Principles 6, 7, 9** IEC 62676-4 Clauses 5.3.9, 10 & 11
10.6.1	1	Recorded material should be suitable for evidential use as required by the courts if it is to be admitted as evidence; it is therefore essential that recorded material evidence maintains total integrity and continuity at all times.	
10.6.1	2	If recorded data is held on an electronic document management system, the system should conform to BS 10008.	
10.6.1	3	Appropriate security measures should be taken to prevent unauthorized access to the system, this will prevent unauthorized or unintentional alteration, disclosure, loss or destruction of recorded material.	

Clause	Item	Content	Reference / comment
10.6.1	4	Data should not be released to organizations outside the ownership of the video surveillance scheme, other than under guidelines referring to the release of information for the purposes of identifying alleged offenders or witnesses, in accordance with the particular control room's policy and procedure.	
10.6.1	5	A hard copy print should not be made as a matter of routine. If such a print is made the person making it should be responsible for recording the full circumstances under which the print is taken, with reasons, in accordance with procedures. Ideally, each print should be allocated a unique number, recorded in the appropriate log.	
10.6.2	1	Recorded material should be stored in a secure environment, so that the integrity of the media is maintained. This includes recorded material that has been requested by the law enforcement agencies or contains a known incident. Controlled access to the recorded material storage area should be strictly maintained. Data that is to be destroyed should be destroyed under controlled operation.	
10.6.3	1	The recorded material register should show the life of the media at all stages whilst in the owner's possession; such a register may also show itself to be useful in enabling evaluation of the video surveillance scheme. The register should include the following: • Unique equipment reference number • Time/date/person removing equipment from secure storage for use • Time/date/person returning equipment to secure storage after use • Remarks column to cover additional points (e.g., erase/destroy/ handed over to law enforcement agencies/removed from recording machine) • Time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned • In the event of a non-automated system of erasure of data, the time/ date/person responsible for erasure and/or destruction	
10.7		**Databases**	**SCCoP Guiding Principle 9**
10.7	1	Whenever a VSS is used in conjunction with a database it is essential that the database is maintained, accurate and up to date. The source of any information should be assessed for accuracy before use. The database should comply with all relevant legislation including compliance with the Data Protection Act. A policy should be in place to ensure the information is accurate.	
10.8		**Exporting Recordings**	BS EN 62676-4 Clause 11
10.8	1	When exporting recordings the following procedure should be followed: • Maintain records of the operator(s) of the equipment. This enables the manager to establish who was operating the equipment at any given time. • Record without interruption, wherever practicable. Any interruption should be logged.	
10.8	2	The export of data should conform to the Digital Imaging Procedure and UK Police Requirements for Digital CCTV Systems.	

Clause	Item	Content	Reference / comment
10.9		**Review of Operational Needs**	**SCCoP Guiding Principle 10**
10.9	1	The system owner should conduct a review at regular intervals not exceeding 12 months to: • Ensure any changes in the operational requirements of the VSS are identified. • Identify any system improvements that could enhance the system's ability to fulfil the operational requirements.	
10.9	2	It is recommended that the security company providing design input and/or maintenance of the system are involved in any review and that any identified changes are recorded, together with an agreement detailing any work to be carried out.	
10.9	3	Where changes are identified that may remove the need for CCTV surveillance it is recommended that the need to continue surveillance is considered in respect of regulations (e.g. Protection of Freedoms Act, Human Rights Act, etc.).	

Annex B – Overall flowchart:



Annex C – Surveillance Camera Code of Practice – 12 guiding principles

Principle	Cross reference to clause of the SCCoP
1. 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.	6
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.	6.7
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.	6.7
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.	8.4
5. 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.	10
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.	10.6
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.	10.6
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.	3
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.	10.2 / 10.6
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.	10.9
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.	10.7
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.	10.7

Annex D – Further detail of Regulations & Acts of Parliament of potential relevance to VSS

Note: The relevance of these may depend on the particular application. It is normally the system owner/operator that is responsible for ensuring compliance.

The Data Protection Act (DPA)

The Data Protection Act 2018 controls how personal information is used by organisations or businesses.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR).

Everyone responsible for using personal data (including recorded images or video) has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Generally, video surveillance is employed to view and/or record activities of individuals, therefore, most uses of VSS by organisations or businesses will be covered by the DPA. The Information Commissioner's Office has produced 'In the picture: A data protection code of practice for surveillance cameras and personal information' that will assist organisations or businesses greatly on how to ensure that their VSS and operation comply with the DPA.

Key points in the Information Commissioner's 'In the picture: A data protection code of practice for surveillance cameras and personal information' relating to privacy include, but are not limited to, the following:

- Equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the video surveillance scheme.
- Where a fixed surveillance camera faces outwards from an individual's private domestic property and it captures images of individuals beyond the boundaries of their property, particularly where it monitors a public space or neighbours' gardens the recording cannot be considered as being for a purely personal or household purpose and the DPA could apply.
- If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered.
- Operators must be aware of the purpose(s) for which the scheme has been established.
- Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed.
- If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces that are not intended to be covered by the video surveillance scheme.

The Regulation of Investigatory Powers Act 2000 predominantly includes requirements restricting covert monitoring. There is an associated **Covert Surveillance and Property Interference Code of Practice** published by the Home Office. There is also reference to this in The Protection of Freedoms Act 2012, Part 2 Chapter 2.

The Protection of Freedoms Act 2012 includes requirements to be followed in Part 2, Chapter 1. As currently applied, this is limited to cameras operated by police and local authorities. There is a related Code of Practice for Surveillance Camera Systems.

Statutory Instrument 2015 No. 596: **The Town and Country Planning (General Permitted Development) Order (England) 2015,** Part 2 (Class F) Closed Circuit Television Cameras includes restrictions to the location and quantity of cameras. Other parts of the planning regulations may be relevant and advice should be sought from the planning authority.

The Clean Neighbourhoods and Environment Act 2005 has regulations relating to the effects of light and noise pollution on the local environment. This would include lighting used for the benefit of CCTV.

The Human Rights Act 1998 (HRA)
The HRA implemented in the UK gives fundamental rights and freedom to everybody, this Act is based on the European Convention on Human Rights (ECHR) and in Article 8 it states that: “Everyone has the right to respect for his private and family life, his home and his correspondence”.

The Private Security Industry Act 2001 includes requirements for Operator Licensing. **The Security Industry Authority (SIA) issue a CCTV (Public Space Surveillance) Operator Licence.** This licence is required when video surveillance is used to monitor the activities of a member of the public in a public or private place; or identify a particular person. It excludes the use of CCTV solely to identify a trespasser or protect property and is required only if the service is supplied for the purposes of, or in connection with, any contract to a customer.

Statutory Instrument 2007 No. 3486 – **The Civil Enforcement of Parking Contraventions (Approved Devices) (England) Order 2007** and the associated document **Civil Traffic Enforcement Certification of Approved Devices 2008** include requirements that are applied to cameras used for the monitoring of vehicles.

The following Acts of Parliament may apply in specific circumstances:

- The Regulation of Investigatory Powers Act 2000
- The Criminal Justice and Public Order Act (1994)
- The Police and Criminal Evidence Act (1984)
- The Protection from Harassment Act (1997)
- The Criminal Procedure and Investigations Act (1996)
- The Magistrates Court Rules (1981)
- The Magistrates Court Act (1980)
- The Criminal Procedure Rules (2020)

The enforcement of traffic regulations by CCTV may also be regulated (in specific circumstances) by:

- The Road Traffic Regulation Act 1984
- The Traffic Management Act 2004
- The Road Traffic Act 1991
- London Local Authorities Act 1996 (as amended)
- London Local Authorities Act 2000
- Statutory Instrument 2001 No. 690 The Transport for London (Bus Lanes) Order 2001
- London Local Authorities and Transport for London Act 2003

Note: There is a ‘Guide to the Regulation of Surveillance’, this guidance has been drawn up by the commissioners whose work it describes to explain their roles and responsibilities in relation to surveillance matters. This is available from the government website, see: https://www.gov.uk/government/publications/guide-to-the-regulation-of-surveillance

Annex E – Screen size and position

Screen viewing distance

When choosing screen size and viewing distance there are several considerations. Firstly there is a difference between whether a screen is being watched "live", being used to watch recorded images over a long period or if perhaps a small section of screen is being looked at closely to determine specific parts of a view (e.g. to see a logo on a suspect's clothing).

Traditionally for PAL TV screens a general rule stated that the viewing distance be between 3 to 5 times the screen diagonal size. This rule does not necessarily apply for other screen resolutions.

The following table shows the recommended relationship between screen size and distance for normal viewing.

Viewing Distance	Equivalent size for a minute of arc (see text below)		Size of monitor (diagonal inches)*			
Metres	millimetres		PAL TV (equiv. 400x720)	720x1280 pixels (720p)	1050x1400 pixels (SXGA+)	1080x1920 (1080pHD)
	@0.8 minute	@1 minute				
1	0.23	0.29	8 - 9	13 - 17	16 - 20	20 -25
1.5	0.35	0.44	11 -14	20 - 25	24 - 30	30 - 38
2	0.46	0.58	15 -19	27 - 34	32 - 40	40 - 50
2.5	0.58	0.73	19 - 24	33 - 42	40 - 50	50 - 63
3	0.69	0.87	22 - 28	40 - 50	48 - 60	60 - 76
3.5	0.81	1.02	26 - 33	47 - 59	56 - 70	70 - 88
4	0.92	1.16	30 - 38	53 - 67	63 - 80	80 - 101
4.5	1.04	1.31	34 - 42	60 - 76	71 - 90	90 - 113
5	1.15	1.45	37 - 47	67 - 84	79 -100	100 - 126

1 minute of arc = 1/60th of a degree

* A range of sizes is shown corresponding to values equating to 0.8 minutes of arc to 1 minute of arc. The sizes are rounded to the nearest inch.

Note on 4K monitors: *When viewing 4K images on a small screen (e.g. 50 inches diagonal or less), the ideal viewing distance is approximately 1.5m. If the viewing distance is increased passed 1.5m then the 4K imagery will effectively appear identical to that on an HD display. With 4K imagery on a larger screen (e.g., 80 to 105 inches diagonal), the ideal viewing distance would increase to approximately 4.0m.*

In addition, it is important to note that optimum viewing quality will only be achieved if the resolution of the camera is matched by that of the viewing screen. For example, an SXGA+ view (of 1050 x 1400 pixels) shown on a 1080p screen (1080 x 1920 pixels) either involves leaving a border around the edge of the screen or processing to fill the screen which may distort the view and/or involve adjusting pixels to create an approximation to the view because of the need to expand 1400 pixels to be displayed on 1920.

Traditionally the eye test developed by Herman Snellen (which will be familiar as the one used by most ophthalmologists) is based on the principle that the human eye can distinguish detail to one minute of arc (i.e. 1/60th of a degree). "20/20" vision under the test means that the reader can see text that occupies 5 minutes of arc which is 8.87mm at 20 feet. In equivalent terms for viewing a screen with a digital image this means that one pixel should be at least one minute of arc in size from the viewing position. Other research has shown that typically people can actually see detail occupying 0.7 or even 0.3 minutes of arc. It is suggested that display equipment is positioned so that a person watching the screen for long periods are at a distance where one pixel is not smaller than 0.8 minutes of arc.

At the other extreme the total width of view that a watcher should be looking at should not be too wide. Whilst humans can see nearly 180° the extremities of this are not practical and the limits of normal vision should be within 30° above and below horizontal and similarly left and right of straight on. For an operator this could apply to a single screen or a bank of screens. For example, if there are three screens arranged horizontally then they could occupy no more than 20° each.

Note that if we position a display at the optimum (0.8 to 1 minute of arc per pixel) position then no more than two HD displays can be placed in a horizontal alignment and still achieve comfortable long term watching (because 1920 pixels is equivalent to 32° width). In PAL TV terms 5 displays can be arranged horizontally. For high-resolution monitors, if it were all right for an operator to see less of the detail during normal viewing (and check the detail for shorter periods) then a seating position further from the monitors would be acceptable.

These considerations apply to monitors that are being watched over long periods. If a view is to be studied in more detail, then it may be acceptable for the observer to be far closer.

*For comparison 0.8 minutes of arc equates to the sizes at the distances shown in the table above. If a monitor of greater size is used, then individual pixels will be obviously visible. For example, there is little point in viewing a 37 inch 1080p HD screen from a distance closer than 1.5m to 2m. This same table can be used to give the maximum distance from a monitor if the intention is to study a view to see maximum detail. Any gre*ater distance will reduce the detail visible in the view.

Target View Angle

The following table indicates the suggested size as a percentage of the screen for the different purposes (see 6.5). This assumes that the distance from the screen is approximately that given in the table above. BS EN 62676-4 contains a version of this table with more sizes.

Percentage of Screen Height by Purpose

Purpose	Screen Size			
	PAL TV (equiv. 400x720)	720x1280 pixels (720p)	1050x1400 pixels (SXGA+)	1080x1920 (1080pHD)
Monitor	5 %	5 %	5 %	5 %
Detect	10 %	10 %	10 %	10 %
Observe	25 %	15 %	10 %	10 %
Recognise	50 %	30 %	12 %	10 %
Identify	100 %	60 %	50 %	40 %
Inspect	400 %	250 %	200 %	150 %

There is a difference between the size of the screen and the use of the screen. In 6.5 it was suggested that a number of different purposes could be assigned to a camera view when designing the system. This included purpose labelled as monitor, detect, observe, recognise, identify and inspect. The ability to achieve these purposes can be different depending on whether the images are being watched as they occur, watched from a recording or being studied in detail. For studying a recorded view in detail, the image level can be equated in terms of pixels whereas for watching live images there is a minimum screen percentage that applies in preference to the pixel height.

For example in order to perform live monitoring of a public square to see if a person is moving across it, it would be recommended that the height of a person in the view should be no less than 5% of a PAL screen (or 20 pixels in equivalent terms) however if an observer is watching a 1080p screen they would still need the person to occupy 5% of the height although this is now 54 pixels. Alternatively if a recorded image is being reviewed to identify an individual the recommended height for a PAL screen is 100% (or 400 pixel equivalent) but because of greater quality this can still be 400 pixels on a 1080p screen (i.e. 40% of the height).

Annex F – Commissioning checklist for VSS

Company Name: Company Address:

Customer: Site: Site ref: Date:

CHECKS TO BE MADE	CONFIRM CHECK (✔)	CHECKS TO BE MADE	CONFIRM CHECK (✔)
Check the installation is in strict accordance with the agreed specification (*and/or Customer Operational Requirement document) and is to a high standard of workmanship.		*Check that physical guards are in place protecting against tamper and vandalism secure	
Check that the system complies with current industry standards, e.g. BS EN 62676-4, inspectorates' code of practice. ***Note: The agreed specification should state the standards to which it is installed.***		*Check that anti-climb measures in place and effective	
*Check the installed system meets the requirements in the agreed system test plan (where used/agreed with the customer).		*Check that external components are protected against water and dust ingress	
Check cables are installed as recommended by the equipment manufacturer(s)		Check the supply voltage is correct to all parts of the system. Record the voltage of all Extra Low voltage equipment. i.e. Cameras, PSUs etc.	
Check that all installed cables are fixed and supported in a way that they will not be liable to premature collapse in the event of a fire (i.e. cables on the surface and in false ceilings)		Check the system continues to operate correctly when the mains supply is disconnected (if stand-by power supply is specified / used).	
Check that power, signal and data cabling is suitably segregated and insulated		Check the correct operation of all monitoring, multiplexing, switching & recording equipment meets the agreed specification, including image quality & image export requirements.	
Check all wiring is correctly terminated and connections are secure		Check privacy masking zones are set up as agreed / where appropriate, and in accordance with the agreed specification.	
Check that glands and grommets in place and secure		*Check ancillary equipment such as lighting & movement detectors are functioning correctly.	
Check all cables are labelled correctly		*Check all interfaces to alarms trigger the correct camera, preset and recording modes.	
Check that all cable measurements/readings are complete and documented		Check appropriate warning notices have been provided and affixed, as necessary.	
*Check that mechanical protection (for cabling) is in place and secure, e.g. trunking, conduit, or ducts		*For remote monitored surveillance systems, check with the remote monitoring location for image quality, recording, receipt of alarms etc. ***Note: For detector activated VSS, BS8418 applies.***	
Check that cabling around articulated and moveable points on masts and towers protected during movement		Check that warning signage and labels provided secure, visible and accurate	
Comments/outstanding works:			

* where applicable

Technician Name: Technician signature: Date:

Annex F – Commissioning checklist for VSS (continued)

Company Name: | Company Address:

Customer: | Site: | Site ref: | Date:

CHECK FOR EACH CAMERA (TICK ✔ WHEN COMPLETED)	1	2	3	4	5	6	7	8	9	10
a. Check correct camera & lens combination fitted. Field of view and image quality in accordance with the agreed specification										
b. Focus & iris adjusted correctly for all intended light levels. Check through appropriate monitor (s) for image quality										
c. Check correct operation of functional cameras (e.g. PTZ, wash/ wipe, zoom, focus) for free movement with no obstructions										
d. Check privacy masking zones are set up correctly (where agreed)										
e. Check correct setting of all pan / tilt / zoom limits										
f. Check all presets operate to agreed specification										
g. Check & measure voltage (ELV) at the camera and check for correct termination of wiring										
h. Check correct alarm interface triggering including alignment / range / sensitivity of associated detection devices										
i. Check warning labels in place for cameras subject to sudden movement / mains supply warnings										
Comments/outstanding works:										

Technician Name: | Technician signature: | Date:

Annex G – Customer VSS handover & acceptance

Company Name: Company Address:

Customer: Site: Site ref: Date:

CHECKS TO BE MADE	CONFIRM CHECK (✔)	COMMENTS
The system has been installed in accordance with the agreed specification (*and customer Operational Requirement document).		
The designated user(s) has received a demonstration and instruction on the correct operation of the system including any adjustable features.		
All documentation in accordance with the standards to which it is installed, e.g. BS EN 62676-4, inspectorate specific codes of practice.		
The correct documentation has been provided to enable the system to be operated correctly.		
The management and use of all means to access the systems applications and operating systems, including any permissions to remotely access the system, have been implemented as agreed with the customer.		
*Reference images obtained during the test and commissioning process have been provided to the customer.		
A system logbook has been provided and an explanation of how to record / report events given.		
Contact details for summoning assistance have been provided in the logbook and their use explained to the user.		
For remote monitored surveillance systems, procedures for summoning support and any agreed requirements have been explained to the user.		
Any security code numbers, keys and software license details have been issued and explained to the user.		
Privacy masking zones have been set up as agreed and information on compliance with current data protection legislation has been provided.		
All surplus materials and equipment are cleared from the site and the premises have been left clean and tidy.		
Comments/outstanding works:		

* where applicable

Technician Name: Technician signature: Date:

I confirm that the VSS has been installed to my satisfaction, and that the premises have been left in a tidy condition and that I have received:

1. Demonstration showing compliance to the agreed specification (inc. the OR) and system test specification
2. Full and comprehensive written operating instructions for the system
3. Training & instruction in the operation of the system
4. A VSS handbook and logbook has been explained and duly completed with contact details for summoning support

Customer Name: Customer signature: Date:

Annex H – Police form

Sample form for supplying information to Police forces

Some Police areas maintain information about VSS installations to enable easy location of systems that may have information for investigative and evidential use. A form such as the following may be completed by the installer to assist the system owner if such information is requested by police.

VSS Details

Premises
Company name:
Premise type:
Address:
Town:
Postcode:
Tel number:
Key-holder(s):
Installer:
Email:
Camera & system details (include sketch plan showing positions and angles)
Internal cameras:
External cameras:
Model number / name:
Make / manufacturer:
Other system details:
Any other comments:
Hard drive capacity (equivalent hours approx.):
Retention period:
Quality (recorded resolution):
Playback method:
Camera view:
Grid references:
For Police use only
BCU:
NPU:

NOTES

About the BSIA

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.

This document was created by the VSS Section of the British Security Industry Association (BSIA).

VSS has had a profound impact on crime prevention and detection. The UK leads the way in the application of CCTV and its use is wide-ranging, encompassing facial-recognition technology, remote video monitoring, video smoke detection, mobile systems and Automatic Number Plate Recognition as well as many other functions.

In order to provide guidance and simplification in the complex area of VSS, the BSIA is very active in the European & International standards arenas and also develops its own guides and codes of practice where currently standards do not exist.

The VSS section encourages debate on new developments and concerns, such as digital video evidence and facilitating communication protocols between different manufacturers' products. In doing so it seeks to ensure that all stakeholder interests are represented including security companies, users, the police, inspectorates and insurers. The section also works with government on these issues.

VSS must be operated responsibly in order to respect citizens' rights and maintain public confidence. Laws such as the Data Protection Act have an important role to play in achieving this. BSIA VSS companies drive best practice in this area and can provide advice on how VSS users can adhere to the relevant legislation.

BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well- represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

BSIA Ltd
Anbrian House
1 The Tything
Worcester
WR1 1HD

t: 01905 342 020
e: info@bsia.co.uk
www.bsia.co.uk