SURVEILLANCE CAMERA COMMISSIONER

Surveillance Camera Commissioner Buyers Toolkit

Contents

You can move around this toolkit more easily by using the icons at the bottom of the page as follows:

previous page

last page you looked at

home page/contents

next page

Hyperlinks can be found where words are in green and bold.

Introduction

IS THIS GUIDE FOR ME?

This guide is intended for anyone in any organisation up to and including small and medium sized enterprises buying a surveillance camera system who wants to maximise their chance of success (and minimise risk) by observing the principles of good practice below.

As a buyer, you could have many different roles in an organisation, but there are a few things that you will all have in common:

- you want to feel that you have spent your money wisely
- you want your needs met now and for the life of your surveillance camera system
- you want a solution that solves a problem and may have less interest in the technology used
- you don't want to be an expert in surveillance camera systems
- you want to hire a competent service provider and be able to hold them to account

This simple guide will give you an overview of what you should be thinking about as you decide whether you need a surveillance camera system. For larger organisations, there is a more in depth guide in the Surveillance Camera Commissioner's **Passport to Compliance**. The commissioner's website includes lots of useful information and links to further sources of advice about good practice in the use of surveillance camera systems.

What happened to the term CCTV?

CCTV stands for closed circuit television. It originated when such systems worked on a closed circuit (as opposed to broadcast television which everyone could receive). These days most "CCTV" systems are in fact connected to networks and whilst still popular the term is no longer accurate. Industry standards often use the term *video surveillance system (VSS)* in preference to CCTV. In this guide, we have used the term *surveillance camera system* (or "*system*" for short). A surveillance camera system includes the cameras and all the related hardware and software for transmitting, processing and storing the data which is captured.

Surveillance Camera Code of Practice and Commissioner

The Surveillance Camera Code of Practice is issued by the Home Secretary under the provisions of the Protection of Freedoms Act 2012. The code provides 12 guiding principles which if followed enable an organisation to demonstrate that the operation of its surveillance camera systems is to a lawful and ethical standard in which the public may have confidence. Relevant authorities such as the police and local authorities are required by law to have regard to the code. However, all operators of surveillance camera systems are encouraged to voluntarily adopt its principles.

The Surveillance Camera Commissioner is appointed by the Home Secretary (and as a regulator is independent of government) to encourage compliance with the Code of Practice and provide advice about it. He works with other regulators who have an interest in surveillance and the protection of privacy. He works particularly closely with the Information Commissioner who upholds data protection rights and responsibilities, and holds statutory enforcement powers for those who breach their data protection obligations.

WE WANT TO KEEP THIS GUIDE SIMPLE

This guide has been organised to provide you with the basic information so you can make informed decisions about your need for a surveillance camera system. It is focused around 5 stages required to achieve success shown in the **illustration**.

We've focused on recognised good practice; by which we mean the basics to ensure your needs are met, that you understand the legal requirements, and any potential to interfere with the right to privacy is taken into account.

At this stage it should be pointed out that a surveillance camera system may not be the appropriate solution for you, or at least surveillance camera systems alone may not be the appropriate solution for you and a more suitable solution will need to be pursued. This should become apparent during the 'justify and plan' stage.

To help you get started, we've included some examples of **common mistakes to avoid** in setting up any surveillance cameras, and thought about some **frequently asked questions** and used these as well as a list of contents. We've also included a **glossary** of the most commonly used technical terms to help you understand the jargon you may hear about surveillance camera systems.

Acknowledgments

This guide was prepared as part of the Surveillance Camera Commissioner's **National Surveillance Camera Strategy for England and Wales**.

Its development was led by the British Security Industry Association with input from Tavcom Ltd, Chubb Fire and Security Limited, ATEC, SecureOne, Syntinex, National Security Inspectorate, SSAIB, Lambert Associates, NetVu Ltd/Dedicated Micros Inc, Advent IM, the Centre for Strategic Cyber Security Science, the Information Commissioner's Office, the Home Office Centre for Applied Science and Technology (CAST) and Alasthom.com.

The Surveillance Camera Commissioner is grateful to all these partners for their contributions to the project.

This guide will assist you in analysing your security problem and help you understand what you want a surveillance camera system to achieve, and any privacy implications.

An effective system is one that meets your needs, or solves your problems, does it reliably, and carries on doing it for as long as you need (usually at least 5-10 years). Success starts with understanding what the system is for - its purpose.

Designing a system that will meet your operational requirements and all relevant legal requirements, takes specialist skill and knowledge. A good service provider should be able to walk you through this and then design and install a system that meets it.

Your service provider should prove to you that the system they have designed and implemented has met your operational requirement.

A well designed and installed system should continue to meet your needs reliably for many years. But it will require ongoing maintenance and management.

Over time things change and this has to be factored in and managed. For example, your operational requirement might change, a piece of equipment might stop working or new people may be operating your system.

Stage 1
Justify and plan

- **Define the problem**
- **Risk management**
- **Data protection impact assessment**

Stage 2
Operational requirement

- **Define your operational requirement**
- **Requirements for use as evidence**

Stage 3
Buying your system

- **Standards and certification**
- **Asking for proposals**
- **Installation**

Stage 4
Commissioning and user acceptance

- **Commissioning and user acceptance**

Stage 5
Operating your system

- **Operating your system**

Security problem → **Surveillance that meets your ongoing operational requirement**

Common mistakes to avoid

There are many common mistakes you can make if your service provider doesn't have a clear instruction when you ask them to help solve your security problems.

Here are some examples of what you want to avoid. This guide will help you to get a surveillance camera system installed which meets your needs and is fit for purpose.

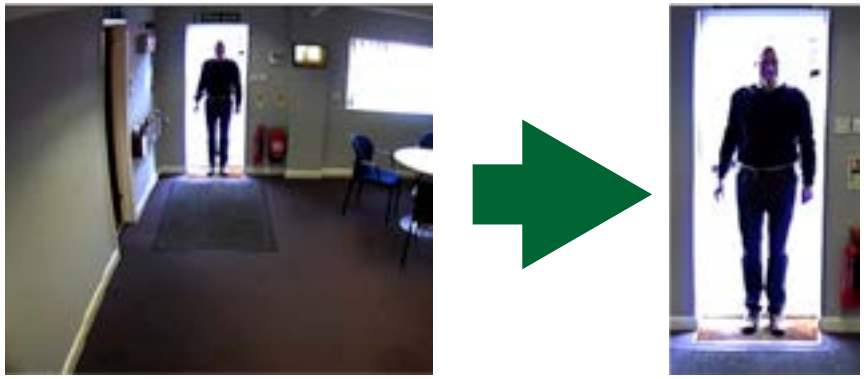
CAMERA POSITIONING

Correct positioning is often overlooked. To gain optimal performance from your surveillance camera system, you will need to consider:

- light sources
- camera height

Don't try to fight light. With correct positioning of the camera you can use the available light to ensure pictures are fit for purpose during day and night.

Remember to watch out for any obstructions such as tree branches, signs or banners. They can ruin your camera view.



Common mistakes to avoid

COMPRESSION

Rapid advances in technology give manufacturers the ability to produce surveillance camera systems which provide high quality images. High quality images do however contain a large amount of data. Here are some extreme examples of image compression, which is often used to speed up the transmission of data or to reduce file size so less storage space is needed.

To give you an idea of the amount of data storage required, one hour of live uncompressed Full HD video footage at 25 images per second equates to about 143 DVDs of storage. So compression is often used to help manage the data.

The level of compression can depend on a number of factors:

- movement in picture
- quality of image (light levels and noise)
- frames per second
- transmission media
- how long you retain images
- quality of recording settings

It has long been suggested that your decision over how many days you need to retain the images will help decide the level of compression of your system's data. A shorter time frame can mean a higher level of quality and frame rate can be achieved in your stored data.

Your retention times should depend upon your **operational requirement** and not be dictated by storage space. Equally, your frame rate compression should be set to meet your operational requirement for that camera.

Remember that a high resolution image which is highly compressed shows similar image quality to a lower resolution image with less compression. It would be pointless paying your supplier for expensive high resolution cameras and then using heavy compression just because you want to save money on storage space.

High resolution Recording

Low compression

Low resolution Recording

High compression

Common mistakes to avoid

CAMERA AND LENS NOT FOCUSED CORRECTLY

Focusing the camera and lens so it remains in focus during both night and daytime operation is vital. Incorrectly focused images will cause issues when recording and zooming in.

When commissioning your system, ensure that the recorded images are also tested, making sure image is correctly focused.

Frequently asked questions

Click on the question to find an answer

- How do I avoid getting ripped off?
- What do I want a surveillance camera system to do for me?
- How do I assess the risks I want to manage using a surveillance camera system?
- Whose privacy could I be invading with my system?
- What is an operational requirement and why do I need one?
- How do I make sure my system can provide evidence to help investigate an incident?
- How do I get what I really need from suppliers?
- What standards should I follow?
- What laws and regulations do I have to follow?
- How do I know my system is fit for purpose it is installed?
- How do I keep my system fit for purpose once it is running?
- What can I do to protect my system from cyber attack?
- What could go wrong?
- How do I understand all the jargon?
- Where can I go for further information?
- What about the new data protection regulations?

Define the problem

The purpose of this section is to help you think through the reason why you might want a surveillance camera system, and whether it is the most appropriate solution to your problems.

Your first step is getting a detailed understanding of the problem, or problems, you are trying to solve. This will help you define your purpose (the problem you want to solve and why). You can then start to assess the options – including a surveillance camera system – and make an informed decision about how best to proceed. Your assessment should include being sure that your use of surveillance is in pursuit of a legitimate aim, is necessary and proportionate to meet a stated purpose, and is compliant with any relevant legal obligations. Only then can you justify your use of surveillance.

CAN I DEFINE MY PROBLEM AND THEN DEFINE A PURPOSE IN SOLVING IT?

Going through the process of understanding your problem will ensure that the key points of what is to be achieved from a new security system are considered, such as: Why do I want a to use surveillance? Do I really need it? What is its purpose? What will it achieve? What will the performance criteria be? What are the objectives?

Unless you have a clear understanding of the causes behind the problem you want to solve, there is risk that any solution you adopt to address it might be ineffective or could even make your problem worse. So spend some time thinking about causal factors. Once you understand the causal factors behind your problem, you can then set objectives to tackle them and write a statement of need.

Without gathering this type of information it will not be possible to measure success or justify your investment.

Example of a statement of need

There is a growing problem with alcohol-related disorder in Anytown city centre during hours of darkness and an associated negative impact on public perceptions of personal safety.

The proposed surveillance camera system aims to support and supplement existing efforts to address this problem by acting as a deterrent to disorder, and recording evidence when it does occur. This will contribute to a reduction in alcohol-related disorder and improve public perceptions of personal safety in Anytown city centre during hours of darkness.

IS SURVEILLANCE THE RIGHT SOLUTION?

A surveillance camera system is undoubtedly a powerful tool which can be used to protect people and assets, and to combat crime. However, with a detailed understanding of the problem that needs to be resolved, it is worth considering if there are simpler, cheaper or less invasive solutions that will address your problem – such as removing the risk, decreasing the vulnerability and reducing the likelihood. These are all items that can be covered in a **risk assessment**.

One specific area of risk which arises with any surveillance camera system is the risk of interfering with people's privacy. Whenever you capture someone's image on your system you are processing their personal data. The collection and storage of data that can be used to identify an individual must be processed fairly and within the law.

Processing such personal data can only be done lawfully by following the requirements of data protection legislation which is regulated by the Information Commissioner. Some big changes come into effect following the General Data Protection Regulation and the Data Protection Act 2018. Under new laws, most surveillance cameras will require a **data protection impact assessment** (DPIA). This should be started at an early stage before installing a surveillance camera system.

Once you have your statement of need, risk assessment and data protection impact assessment, you can now decide how best to proceed. If a surveillance camera system is justified as part of the solution, then read on for advice, guidance and tips on good practice. This will help you in buying a system which is fit for purpose and really does meet your needs.

WHAT IS PLANNING AND WHY IS IT IMPORTANT?

Planning the system will show if the introduction of a surveillance camera system will help solve the problem. The plan should be based upon a risk and threat analysis that has determined that the problem exists and the extent of impact should the problem occur. Your problem must be clearly identified and defined, stakeholders must be consulted and the success criteria must also be documented so that a controlled and measured analysis can be carried out after the introduction of your system. Planning is important because it should help you to address any legal and privacy issues.

To make sure your system does help to solve the problems set out in your statement of need, here are some key issues to consider in your planning process:

- What areas does the system need to cover? Draw up a **site plan** to help you assess where to put your cameras.
- Do I want to be proactive or reactive? A proactive system uses live images to actively monitor an area to predict an event, as a preventative measure or to provide information to support a real time response during an event. A reactive system uses recorded data to respond to or investigate an event after it has happened or, at best, when it has started to happen. This basic operational decision needs to be made during the planning stage because it has an impact on the system design. Does it need display screens or recording capability – or both? A reactive system is likely to need a high-quality recording for a longer archive period than a proactive system which needs a high-quality user interface and operator ergonomics. The decision of whether to favour live or recorded images should be addressed at the planning stage to meet the operational requirements of the system.

- How long should I keep the images? In line with data protection obligations, the retention period for video images should not be any longer than necessary. The retention period for images captured by surveillance camera systems will vary due to the intended purpose for the recording.
- How do I keep the images safe and secure? Access to video images must always be restricted to those who need to see them to fulfil the purpose of surveillance. Anyone with access to your system should know the clearly defined procedures and rules on who can gain access and for what purpose such access is granted. Your system must also be appropriately protected from cyber attacks and unauthorised access. Defining the security for your system, including being able to resist cyber threats, is a key part of your **operational requirement**.
- How do I make sure I can share images as evidence to inform an investigation? Sharing images from a surveillance camera system must comply with **data protection legislation**. If the images are to form evidence in a criminal investigation they must be handled in line with certain procedures for disclosure. If your statement of need includes gathering evidence, your system must be designed and operated to meet **certain evidential requirements**.
- Who do I need to tell about my plans? Good practice includes consulting with anyone who may be affected by your surveillance before you proceed; this should form part of your **data protection impact assessment**. Video images of people are personal data, so you must inform the Information Commissioner's Office that you are processing personal data. Once you start to operate your system, you must inform people that they are under surveillance. An example of a privacy notice to inform people about your surveillance is on this page; further **guidance about the right to be informed and privacy information** is available.

Risk management

INTRODUCTION TO RISK MANAGEMENT

The purpose of this section is to help a buyer to create a basic threat, vulnerability and risk assessment as one of their first tasks in defining the problems where a surveillance camera system might form part of an appropriate solution. The toolkit also includes a **worked example**, from which you will recognise that every risk assesmsent will differ from organisation to organisation depending on its situation and circumstances.

At this stage, your risk assessment does not need to cover the **data processing** and **cyber security** risks arising from use of a surveillance camera system; those risks are covered later on in the project.

It has often been said that risk management is just a new term for what organisations have been doing for many years and that it is simply 'common sense'. We have always sought to avoid the consequences of unpleasant but expected events. Effective security means anticipating the threats and then taking measures to manage the risks.

RISK MANAGEMENT METHODOLOGY

In reality, we will still continue to make common sense judgement calls when time and resources are limited. But the methodology of risk management calls for a more deliberate, systematic approach to our decision-making than just an educated guess.

- Step 1: Identify and assess the risks
- Step 2: Evaluate the risks and decide on control measures
- Step 3: Manage the risks through your control measures
- Step 4: Review your assessment and update as and when necessary

Risk management dictates that we do only those things that can be justified as the result of a systematic assessment of the actual degree of risk in a situation. Money being thrown at issues is not the best way for an organisation to deal with risk in today's competitive climate.

IDENTIFY AND ASSESS THE RISKS

The first problem is that of obtaining information. You will need to know:

Risk assessment elements defined	
Risk	The probability that a particular threat will exploit a particular vulnerability Risk = impact of (vulnerability x threat)
Asset	Any person, facility, material, information or activity that has a positive value to the organisation
Threat	An adverse event with the capability and the intent to violate security
Vulnerability	A weakness within the resources which could, at some point, be exploited by the threats
Impact (consequence)	An evaluated consequence of a particular outcome and might result from the exploitation of vulnerabilities by threats
Likelihood (probability)	The chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors

- What are the assets (people or property) in need of protection?
- How critical are each of these assets?
- What adverse events pose a threat to the critical assets?
- What is the probability or likelihood of each threat occurring?
- What are the site-specific vulnerabilities of these critical assets?
- What are the consequences or impact of the event?

Recording your threats, their likelihood and impact using a **risk assessment** and **risk matrix** will assist in the prioritisation of your risks using each aspect of the risk assessment process.

EVALUATE, MANAGE AND REVIEW THE RISK

How do you manage the risks identified? The costs and benefits of each alternative countermeasure need to be compared. You can then decide on the most appropriate method or countermeasure to manage the risk.

In respect of risk reduction, costs can generally be measured in terms of money, inconvenience, time and/or additional personnel. There are generally 3 means to reduce risks. These are:

- a change in written procedures/policy
- the provision of hardware – remember to consider maintenance costs and subsequent replacement
- the provision of manpower

Review your risk assessment on a regular basis and update when necessary.

FURTHER READING

For more detailed information on risk management refer to:

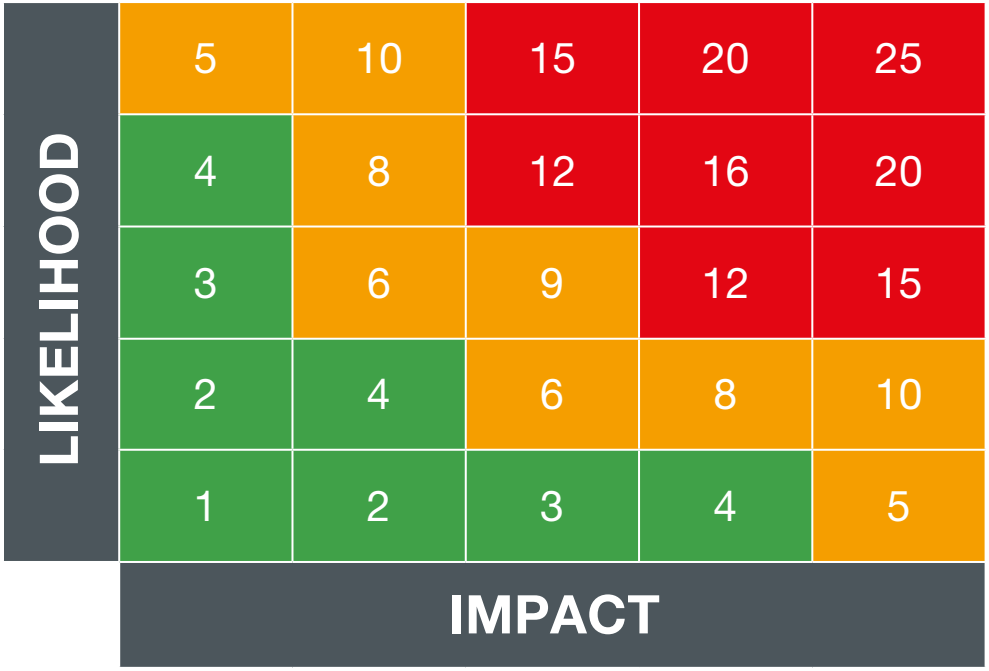
ISO 31000:2018, Risk management – Principles and guidelines

Risk assessment – worked example

Adverse event (threat)	Likelihood	Impact	Risk rating (Likelihood x Impact)	Control measures	Comment
Inappropriate access to hazardous material store due to poor security	4	3	12	Personnel security; pre-employment vetting checks; storage of material in a lockable area; key management	Ensure Control of Substances Hazardous to Health requirements (COSHH) have been adhered to properly
Unauthorised access to grounds due to open plan nature of site	2	3	6	Appropriate signage; perimeter demarcation; security patrols (surveillance cameras/individual)	Improvements to perimeter fencing and access to buildings require improvements
Unauthorised access to buildings due to poor security	3	3	9	Introduce staff pass system; visitor processing/escorting; anti-tailgating training; front door intercom/video module	Encourage staff to challenge unknown personnel not wearing ID
Breach of security due to poor storage of confidential waste	3	4	12	Security procedures in place; staff training; procurement of lockable waste bins	Refresher training for all security personnel should be scheduled regularly
Criminal damage to property due to inadequate physical security	3	4	12	Improved perimeter security; Improved external lighting at night; surveillance cameras; security patrols	Impact can vary considerably: from graffiti, to sabotage, to major arson attack
Lack of ability to investigate an incident due to inadequate processes	1	3	3	Security procedures in place; staff training; incident management exercises	Ensure all investigation staff know how to properly secure evidence

Scores for likelihood and impact	1	2	3	4	5
	Very low	Low	Medium	High	Very high

Risk matrix



Scores for likelihood and impact	1	2	3	4	5
	Very low	Low	Medium	High	Very high

Data protection impact assessment

INTRODUCTION TO CREATING A DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Principle 2 of the the surveillance camera code of practice states that:

> *"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." This reflects data protection obligations set out in data protection law.*

With this in mind it is important for anyone who is contemplating the introduction of a surveillance camera system to be mindful that for most surveillance camera systems there is a mandatory requirement to do a Data Protection Impact Assessment (DPIA). This can completed by the use of the existing **templates and self-assessment tools** available on the Surveillance Camera Commissioner's website, or by incorporating the principles into an existing process reference manual, or by creating your own document.

This is not a one-off exercise. Privacy impact should be reviewed regularly and whenever fundamental changes are made to your system (such as when cameras are added, removed or their view repositioned).

2018 sees some significant changes in data protection law and obligations. If in any doubt, the best place to seek guidance is from the **Information Commissioner's Office**, which has been consulted over the production of this toolkit.

If you decide to process personal data through a surveillance camera system you will be a controller under data protection law. As a controller you will be responsible for completing a DPIA. In doing so, these are some of the important factors to consider:

- effect on individuals
- identifies the responsibilities of people involved in processing data and the Data Protection Officer who you must consult over your DPIA
- review policies are in place
- only required information is held
- images are not stored longer than necessary
- only authorised and trained people can review images and recordings
- any associated information such as databases should be adequately protected

Under the new data protection obligations of 2018, if you are unable to mitigate the privacy risks adequately you have to submit your DPIA to the ICO for review. Do remember that the DPIA process is meant to help you assess whether the use of surveillance is a necessary and proportionate response to solve your problems.

Information Commissioner

The Information Commissioner has a statutory role to promote and enforce rights and responsibilities under data protection laws. This includes powers of enforcement and complaints handling.

The Surveillance Camera Code of Practice draws on and reinforces data protection obligations in relation to video surveillance.

Define your operational requirement

WHAT IS AN OPERATIONAL REQUIREMENT AND WHY DO I NEED ONE?

Whether you are planning a new system or modifying an existing one, the operational requirement (O/R) is the next step in the planning process after your risk assessment has been completed. The purpose of the operational requirement is to clearly identify:

- the area(s) that the system will cover (marked on a **site plan**)
- the level of detail required in the resulting images, normally expressed using defined industry terms like ‘identify’ and ‘recognise’
- the reason for that coverage (taken from the risk assessment) including the target and activity

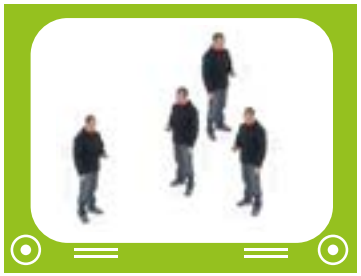
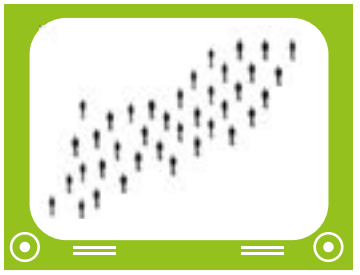
A clear operational requirement is the most effective way to ensure the installed system meets your expectations. It is a powerful tool for the buyer as it:

- provides a clear and mutually agreed instruction to the designer/ service provider
- ensures that the designer/service provider takes responsibility for design and product selection
- provides a basis for validation, the process of user acceptance and confirming that the designed and installed system meets the O/R
- identifies management issues such as monitoring and response to incidents
- provides instructions on privacy and cyber security requirements

To help you get started, we have included a worked example of how you might write a **schedule which sets out your operational requirement for each area of your site plan**. This also includes a checklist for operating issues and system requirements that you and your service provider will need to understand.

PURPOSE OF OBSERVATION

There are 4 generally used categories: Identify, Recognise, Observe and Detect.

Category	Identify	Recognise	Observe	Detect
				
Purpose	Sufficient to identify an unknown person	Sufficient to recognise a known person	Sufficient for general observation but not recognise a person	Sufficient for detection system to pick up
Technically this is at least:	4 mm per pixel or 250 pixels per metre or 100% of the available screen height or 40% Full HD screen height	8 mm per pixel or 125 pixels per metre or 50% of the available screen height or 20% Full HD screen height	16 mm per pixel or 62.5 pixels per metre or 25% of the available screen height or 10% Full HD screen height	40 mm per pixel or 25 pixels per metre or 10% of the available screen height or 10% Full HD screen height

These 4 categories are part of the industry standards which are set out in BS EN 62726-4 2015. We have only illustrated the 4 categories which are usually required as part of a surveillance camera system. There are 2 more, which are not generally used:

Inspect has an image 4 times the size of Identify, and is usually required only where automatic facial recognition is part of the operational requirement

Monitor has an image size half as big as that in Detect, which is more likely to be specified in practice

EXAMPLE OF AN OPERATIONAL REQUIREMENT:

Based on your risk assessment, your operational requirement may look like this:

Front entrance - **IDENTIFY**
anyone entering or leaving

40 % Full HD
4 mm pixel per metre

Zoomed to 100%

Rear entrance - **RECOGNISE**
anyone nearby during office hours

20% Full HD
8 mm pixel per metre

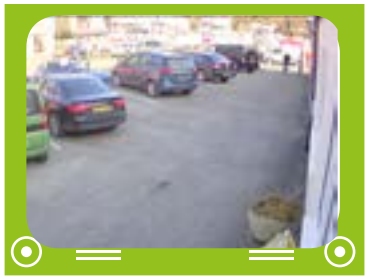
Zoomed 50%

Rear of building - **OBSERVE**
any activity

10% Full HD
16 mm pixel per metre

Zoomed to 25%

Car park - **DETECT**
presence of any people



10 % Full HD
40 mm pixel per metre

OTHER POINTS TO REMEMBER

Operational

It is important to note that there are other factors that can compromise the usability of the resulting images, such as camera noise, blurring or insufficient lighting. The good news is that a professional service provider, armed with your operational requirement will be able to take these into account to ensure your operational requirement is met.

See **Common mistakes to avoid** for examples.

Further advice on the storage of recorded images can be found on the **CPNI website**.

Recording

Most surveillance camera systems are intended to record images for later review. You need to consider how long the images need to be kept. This needs to be long enough to identify that an incident has taken place, and to secure the evidence, noting that the police may be involved in determining what is evidence. You might want to consult your local police for their advice on a proportionate retention period.

The other consideration is quality of image (level of compression), number of images per second (frame rate). Your service provider should be able to recommend a frame rate based on your operational requirement but this will normally be between 3 and 25 images per second depending on the speed of the target and the activity to be captured.

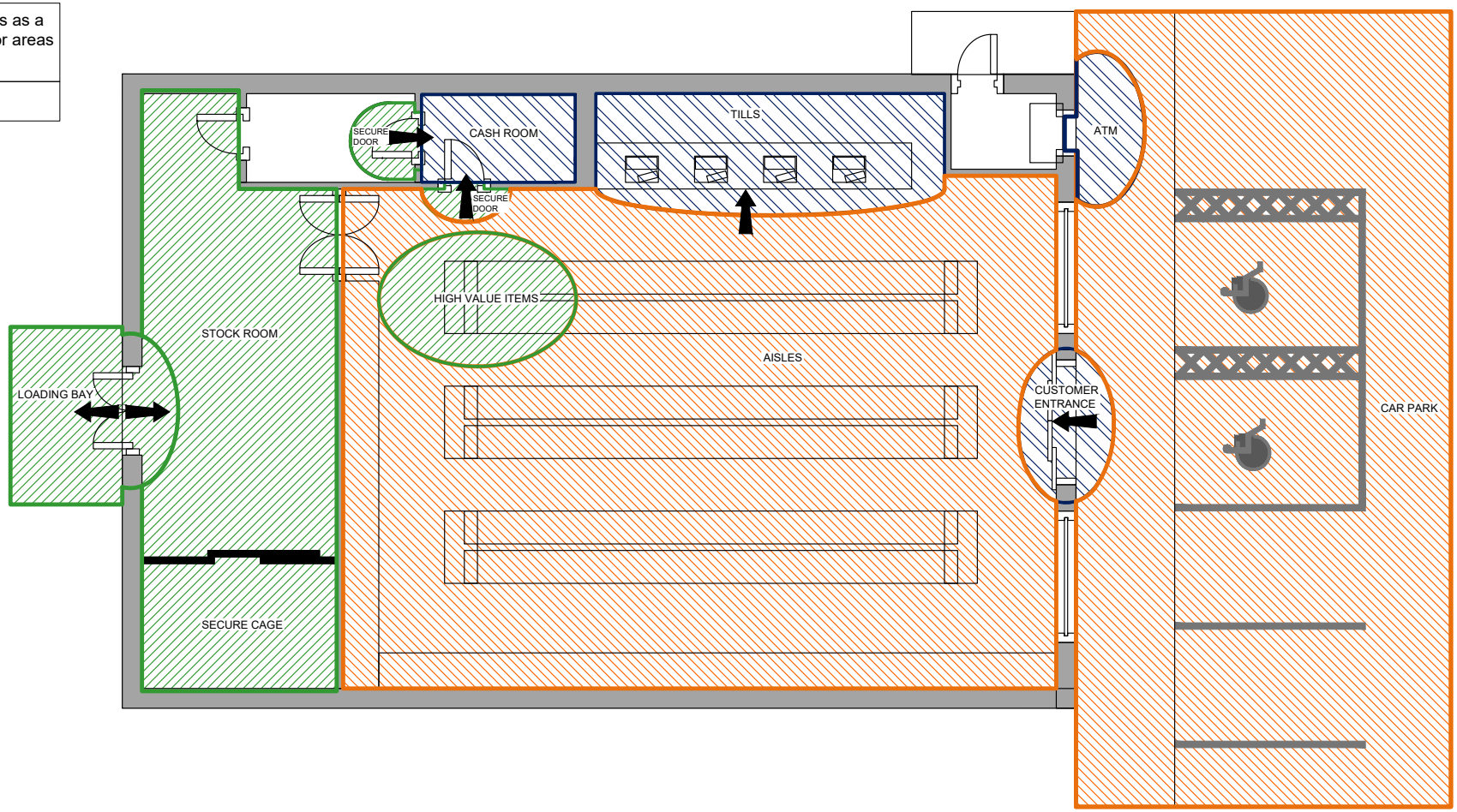
Low resolution recorded image

SITE PLAN EXAMPLE

Operational Requirement - General Observation Categories	
IDENTIFY	Identify
RECOGNISE	Recognise
OBSERVE	Observe
DETECT	Detect

Cameras covering 'OBSERVE' areas as a minimum satisfy the requirements for areas requiring 'DETECT' Levels

➡	Direction of Movement towards the camera



OPERATIONAL REQUIREMENT – WORKED EXAMPLE OF SCHEDULE

FOR RETAIL PREMISES SHOWN IN SCC BUYERS TOOLKIT SITE PLAN

DEFINE THE PROBLEM					
Area description	**Activity**	**Target(s)**	**Purpose of observation**	**Acceptable coverage**	**Target speed**
Describe the area to be covered	Describe the potential activity that needs to be monitored (from risk assessment)	Describe the target e.g. people, vehicles (cars and large lorries)	How much detail do you need in the picture?	Select 100% or 95%, see guidance	How fast will the target be moving?
Customer entrance		People	Identify	100%	Walking
Cash Room entrances		People	Identify	100%	Walking
Tills		People	Recognise	100%	Stationary
High value items (shop floor)		People	Identify	100%	Variable
Stock room		People	Recognise	100%	Variable
Secure cage		People	Recognise	100%	Walking
Loading bay		People, vehicles	Recognise	95%	Variable
ATM (customer)		People	Identify	100%	Stationary
Aisles (shop floor)		People	Observe	100%	Walking
Cash room		People	Identify	100%	Stationary
Car park	Theft from motor vehicles, vandalism, theft of motor vehicles	People, vehicles	Observe	95%	Variable

MANAGING YOUR EXPECTATIONS OF A SURVEILLANCE CAMERA SYSTEM

Think about your expectations from a surveillance camera system. Often people are unaware of the capabilities and complexities of a camera or of the system hardware and software that sits behind it.

Working through the following list will help to clarify what you need from your system, and what additional functionality may help to meet your needs:

- visual deterrent
- live monitoring
- monitoring of persons within the boundary/grounds
- recognition of known person at the building edge
- monitoring vehicles within driveway areas
- identification of unknown individual at the entrance door
- identification of unknown individual at the gate
- view vehicles entering or leaving site via the gate
- speed of intended targets
- internal cameras for high risk or high value stock
- internal cameras for health and safety monitoring of persons
- identification of persons opening fire doors
- expected response
- ease of operation for the end user

This list is not meant to cover every possible requirement, so do add to it with your own specific reasons and site objectives, and consider multiple selections as applicable.

CONSIDER BOTH THE IDENTIFIED AND POTENTIAL RISKS

Studying a site plan drawing will give you an indication as to the physically vulnerable areas, but local knowledge is also fundamental to the threat and risk analysis of a site. Ask yourself the following questions:

- What is the risk you want to monitor with your surveillance camera system?
- Is there a history of theft or disorder or is it in a high crime area?
- Is the location unoccupied for long periods of time?
- Are there security guards present?
- Is any loss or incident likely to have a further impact on your business such as inability to supply customers?
- Are your assets of high value compared to the risk and your investment?
- Are your assets easily removable?

Along with site specific considerations, try to classify each of the risks above as minor, moderate or severe with a view to prioritising the operational requirements.

OPERATIONAL REQUIREMENT – CHECKLISTS

OPERATIONAL ISSUES (LIVE VIEWING)	Specified by buyer
Who monitors	
When monitored	
Where monitored	
What standards will apply	
Response required to incidents	

SYSTEM REQUIREMENTS	Specified by buyer
Alert function	
Display screens	
Retention period	
Recording	
Export/Archive	
Cyber security requirements	

Requirements for use as evidence

In most surveillance camera systems, the recorded video is at least as valuable as a live image. If your system is solely for live monitoring, then you can skip this section. If, however, you think that images from your system may at some point form the basis of a formal investigation (whether that involves the police and criminal justice system or is purely internal) then this section will guide you as to your responsibilities and what you should expect from your service provider.

If you do plan to use images for evidential purposes, you will need to put in place technical and administrative processes that can assure the integrity of your system as a source of evidence.

OVERVIEW

The things you need to consider can be divided into 5 areas:

Area	Principle
Clarity	Image sequences should be clear and contain enough detail to show whether an event happened and who was involved
Storage	Images must be kept confidential, must be original (not altered in any way) and must be available when required
Review	It should be simple to review footage to determine whether the system has captured the event of interest
Export	Once the evidence has been located it should be easy to protect and export it for analysis
Playback	It should be easy for exported evidence to be played back

You should be clear with your service provider that you will require your system to produce evidence, and they should then support you in ensuring these objectives are met.

CLARITY

Objective: Image sequences should be clear and contain enough detail to prove whether an event happened and who was involved.

In the operational requirement you should set out the area and purpose of coverage, activity, target and target speed. Indirectly this sets out the level of detail required, and leaves the service provider responsible for ensuring that it happens.

STORAGE

Objective: Images must be kept confidential, must be original (not altered in any way) and must be available when required.

Retention period – Consider how long you need to keep the images. This should be long enough to ensure that any incidents have come to light, and to locate and secure the relevant footage. You need to be able to justify keeping the images for your chosen retention period. You might want to consult your local police for their advice on a proportionate retention period. If you want to keep your images for longer you should have a clear and documented reason or doing so. A shorter retention period will save money on storage.

Your system should automatically delete images older than the specified retention period. Your service provider should ensure that there is sufficient storage to ensure the retention period is achieved.

Protecting images from deletion – Your system should include the facility to protect images that have been identified as useful to an investigation to prevent them being deleted before they can be exported. Your service provider should allow enough spare storage to accommodate this. We recommend a minimum of 10% of the overall capacity but if you have regular investigations you may need more.

Original images – The validity of images as evidence may be compromised if they have been edited or the file format has been changed.

Capacity – The capacity of your storage system (normally comprised of hard disk drives) should be calculated by your service provider as part of the design process.

Resilience – There are many ways to provide resilience and resistance to failure. Specifying this will increase cost but will reduce the chance of the footage not being there when you need it.

Environment – The storage system should be located in a suitable environment (ideally dust free and temperature controlled) otherwise you are more likely to experience unreliability.

Controlling access – You should ensure that the storage is in an area with restricted access, however having your system in a locked cabinet does not mean its protected from unauthorised access. It is also important to have appropriate logical controls including secure passwords, and if your system is connected to a network, appropriate network security measures.

Audit trail – Ideally the system should keep an audit trail of who accessed what footage and when, and should confirm that the images have not been altered.

Time stamp – The system should include or be linked to an accurate clock. If the time on an image is significantly out it can dramatically reduce the evidential value of images.

REVIEW

Objective: It should be easy to review footage to determine whether the system has captured the event of interest.

You should ensure that the review facilities on the system are practical and suitable for your needs.

Physical environment – If you have an incident it may take some time to locate and review all of the footage, so it should be practical for the reviewer. Ideally, they should be able to undertake this activity whilst sat comfortably at a desk. If your system is networked then this provides flexibility to review from a PC. If the system is self-contained then you will need a dedicated display and access to the recorder controls so the loft, or a cupboard may not be the best location.

Review features – Video surveillance systems may include a range of features that make it easier and quicker to review footage, ranging from skipping periods of no activity, to automatically highlighting specific events using “intelligent” analytics. Ask your service provider for a demo of their proposed features.

EXPORT

Objective: Once the evidence has been located it should be easy to protect and export it for analysis.

Support for external media – You will need to export to something, so your system should support the connection of external media either plugged into the storage device, or to the download PC.

Clear and simple instructions – It is good practice to have clear and simple instructions for exporting footage available, including who to contact for passwords. Consider laminating this and keeping with the system.

Exports additional information – In addition to the video the export should include the software required for playback, and an audit trail showing who exported the images and when.

Native export – It is best if the images are not processed for export. Common video player formats (for example windows media player) can be convenient but are not primary evidence. For that you need an exact copy of what was originally recorded.

Time taken to export – Export of medium and large volumes of recorded video/data can take a substantial period of time. The service provider should advise the approximate times to export short (such as 15 minutes), medium (such as 24 hours), and large (up to all of the data on your system) amounts of recorded video/data.

Recording shouldn’t be affected – Whilst the export is in progress the system should continue to operate normally and unaffected by any extra processing or network load.

Seizure – In a major incident (such as involving loss of life) the police may require a large volume of images. If your system makes this difficult they may seize your recording system to protect the evidence.

PLAYBACK

The replay software must allow the investigator to search the recorded video/data effectively and see all the information contained in the video and any associated data, therefore the playback software should:

- have variable speed control including frame by frame, forward and reverse viewing
- display single and multiple cameras and maintain aspect ratio i.e. the same relative height and width
- display a single camera at full resolution
- permit the recorded video/data from each camera to be searched by time and date
- allow printing and/or saving of images with time and date
- allow the time and date associated with each video to be clearly legible

It should be possible to replay exported video/data files immediately such as no re-indexing of files or verification checks.

FURTHER READING

More detailed guidance on how to do this can be found in **Home Office CCTV Operational Requirements Manual 2009, 28/09 and the Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems V2.0 66/08.**

Standards and certification

Once you understand your operational requirement, it is worth thinking about the approved standards which are recommended before you go ahead and start asking for proposals. Principle 8 of the surveillance camera code of practice says:

> *"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."*

IF YOU WANT A VIDEO SURVEILLANCE SYSTEM, WHAT STANDARDS SHOULD YOU FOLLOW?

There are many approved standards which inform good practice in the operation of a surveillance camera system. Some of these are about technical requirements and others relate to management procedures and processes. Many are developed by the British Standards Institution (BSI) or have been adopted at international level. As part of his statutory remit, the Surveillance Camera Commissioner (SCC) publishes a list of **recommended standards for the surveillance camera industry**.

WHY SHOULD YOU CONSIDER THEM?

Standards are an agreed way of doing things. They can give you a set of tools with the potential to help you perform better and meet your goals. Any organization that follows and implements standards wisely can cut costs and reduce the risk of things going wrong.

There is no legal requirement to follow these standards. Yet if you want to be sure you have a system which is fit for purpose and really does meet your operational requirement these standards will help you to do so. That is why they are recommended.

ARE THESE STANDARDS FOR ME OR MY SUPPLIERS TO MEET?

Your supplier is the expert and you need to be satisfied they understand the standards and are able to demonstrate that they follow the standards.

As part of the SCC's national strategy work is underway to put in place certification against a range of recognisable standards for consultants installers, designers and surveillance system operators. You can find out more about **recommended standards** on the SCC's website..

Third party certification is best done independently by a **UK Accreditation Service (UKAS) accredited certification body**. UKAS is responsible for determining, in the public interest, the technical competence and integrity of organisations across a wide range of sectors. Its remit covers the certification of alarm and security system installers, and the certification of individuals working as security professionals. These bodies include the National Security Inspectorate (NSI) and the Security Systems and Alarms Inspectorate Board (SSAIB).

WHAT ABOUT STANDARDS TO PROTECT ME FROM CYBER THREATS?

Cyber threats are changing all the time, and any surveillance camera system can be vulnerable to cyber attacks which interrupt service or lead to the unauthorised disclosure of images and information. Service interruption could leave you exposed to the very risks you want to manage. Unauthorised disclosure could infringe privacy, break data protection rules or cause reputational damage to the organisation which has been attacked. There is a **Cyber Essentials** certification process that can give you protection against a wide variety of the most common cyber attacks.

Do ask your potential suppliers if they can demonstrate that all their system components have been designed and manufactured to mitigate these threats, and meet Cyber Essentials standards and requirements.

Asking for proposals

If you are contemplating the purchase and installation of a surveillance camera system you need to think about the following important considerations. This short process is valuable regardless of the size of your project and should be considered before entering into any agreement.

Surveillance camera systems can be expensive. So you need to make sure you know what you are getting for your investment and that you have selected the right service provider who can meet your needs.

By following the headings below you should be able to gain a better understanding of what you need and how you imagine it will operate, and be able to explain it to your prospective service providers.

Scope out your operational requirement

What is it you need surveillance to do for you? The overriding purpose of an **operational requirement** is to ensure that you receive the surveillance camera system that was designed for your specific purpose and suits your explicit needs and you can operate successfully. In drawing up your operational requirement, you will have thought through your needs and expectations about the threats and risks that are present.

This forms the basis of an agreement between you and the chosen service provider. It should always include a **site plan drawing** showing each actual camera view required, supported by a schedule setting out the **capabilities and features of the system**. It should ensure that all parties share the same understanding of the expected views from each camera, the lighting conditions and how the system operates. It should also include maintenance arrangements. Your operational requirement can also set out your needs for ongoing protection against cyber attack and unauthorised access to images.

Ask your prospective service providers to explain any shortcomings in the terms of features offered in their proposal. For example, relating to the system's ability to operate in adverse weather or other environmental conditions.

Technical, environmental and commercial factors

Define what you want your system to do and then get your prospective service provider to explain which of the current technologies meet your need and why. Many of the features within high end cameras and systems, such as edge recording or video content analysis, or even video analytics such as automated facial matching may only be suited to very specific operational requirements. Be sure to take an approach that matches the costs and privacy impact of the equipment and camera or system capabilities with the essentials of your operational requirements for each individual camera's area of view.

There is no need to over-engineer the features of a camera or any other system component. Doing so may interfere with privacy and may not be good value for your investment.

Use our jargon-busting **glossary** to assist with terminology. Don't be afraid to challenge your service provider if you need clarification of the technical terms they use or of any features in their system proposals.

Your system should be installed to the **current standards**. In particular you might look out for BS EN 62676 Video Surveillance Systems and BS8418 Detector Activated Remotely Monitored CCTV Systems.

Make clear your expectation that any installation should be neat and tidy with all cables having sufficient protection, especially in vulnerable areas.

Your system will be processing personal data so you must register it with the ICO, and you must ensure there is adequate signage to tell people that they are under surveillance. Ask you service provider to show you an example of the signage they propose to use, and how it meets your data protection obligations. The ICO has prepared guidance on **Privacy by Design**, which is an approach to projects that promotes privacy and data protection compliance from the start..

Selecting and engaging a reputable service provider

You should obtain systems proposals from at least 3 service providers. Once your operational requirement is established, it should be the foundation of comparison when you look for that competent installer to be your service provider. It will also ensure a 'like for like' platform for comparison, and establish the basis of a contract to ensure you get what you expected and it works in a way that satisfies your needs.

Always investigate the credentials of prospective service providers. Companies who achieve and retain registration with UKAS accredited certification bodies such as the **National Security Inspectorate (NSI)** or **Security Systems and Alarms Inspection Board (SSAIB)** are more likely to provide a consistent approach as the service provider is regularly audited by their certification body.

Remember to ask about the expected lifecycle of a component such as a camera and whether replacement parts be readily available if one fails, what is the expected replacement time and will this impact on your ability to continue your operations.

To ensure you get the system you need it is good practice to question the potential service provider on all aspects of how they will manage your installation. This will help give you the confidence that the service provider you choose can meet your needs.

Questions to discuss with each of your prospective service providers once your have their proposals

This list is not meant to cover every issue in the proposals to meet your operational requirement. Yet it will help you to test out each proposal and understand how they meet your needs and compare with each other.

- Fields of view – **What scene will it be looking at?**
- Duration of storage – **How long do I really need to keep recordings for?**
- Target distance – **How far from the camera is the intended target?**
- Target size - **Am I looking at people or cars or other sizes?**
- Target speed – **How fast will the target move (walking or fast car)?**
- Lighting availability – **Do I need addition lighting?**
- Image transmission – **What cable is already available (analogue or IP)?**
- Analytical, motion detection or VCA – **Do I need these features?**
- Monitor, detect, recognise, identify – **What do I want to see?**
- Expected lifecycle – **Warranty periods?**
- Overall number of cameras – **Will I see all the intended targets?**
- Power requirements – **Mains required or PoE network?**
- Weather protection – **Consider the ingress protection rating suitability?**
- Vandal resistance – **The physical protection at the camera location?**
- Aesthetic value – **What will the cameras look like?**

- Compatible replacement – **Is the hardware sustainable or futureproof?**
- Suitable spares – **Are additional future cameras compatible?**

Assistance and legislation guidance

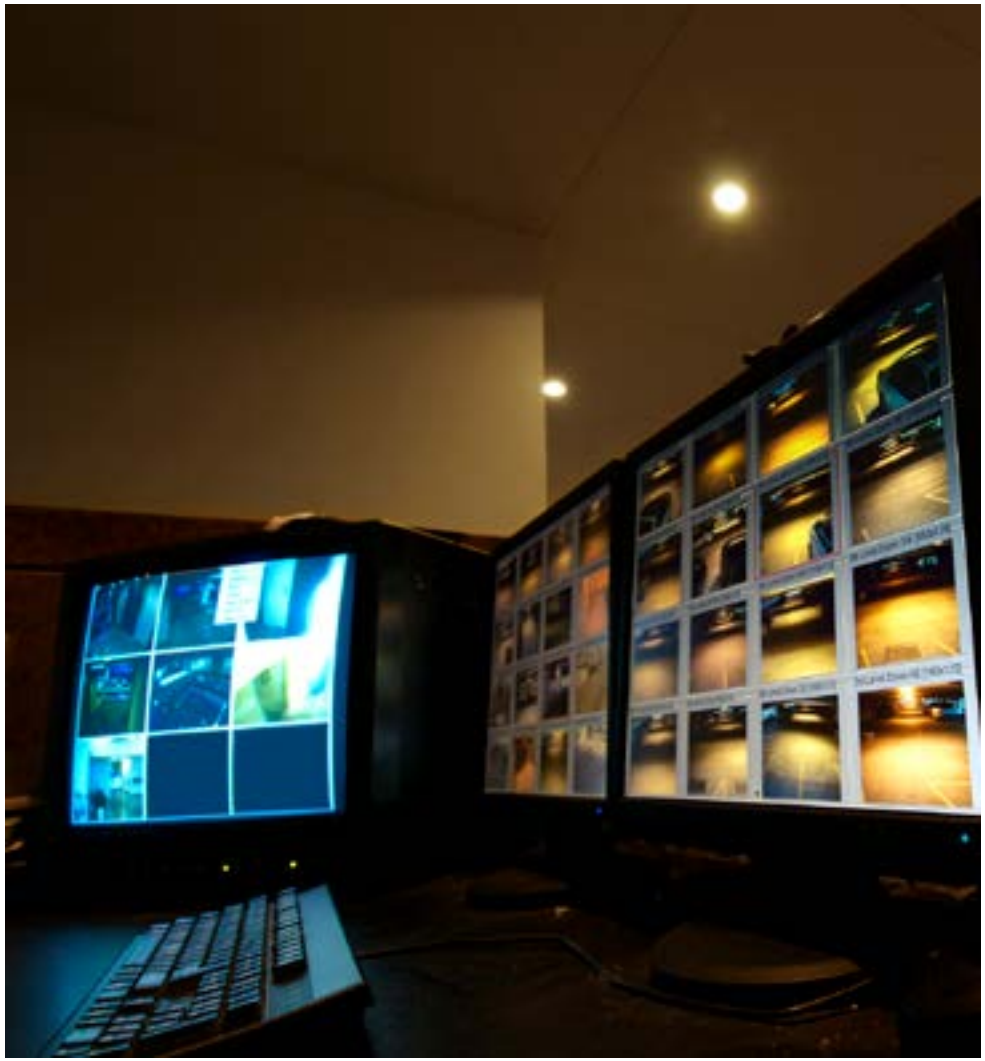
There is an ever-changing list of potentially affected legal acts of parliament, industry approved system guidance documents and general online help available form the following websites:

Surveillance Camera Commissioner
https://www.gov.uk/government/organisations/surveillance-camera-commissioner

Surveillance camera code of practice
https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

Information Commissioner's Office
https://ico.org.uk/

Centre for Protection of National Infrastructure
https://www.cpni.gov.uk/cctv



Installation

Having now decided on your required surveillance camera system and placed an order with your appointed installer, it is important to manage the installation of the system to ensure that it does meet your needs and expectations.

BEFORE STARTING ON SITE

As with any contracted work, there may be disruption to your business. So before the work starts it would be best to have the following:

- a full method statement detailing the planned work
- time scales of installation with agreed dates.
- notification of intended working hours, potential noise etc.
- health and safety documentation including:
  - risk and method statement
  - potential access issues
  - working at height, scaffold or cherry pickers
  - notification of any asbestos concerns
- agreed method of communication for any variations or alterations which deviate from original scheme
- list of names, including sub-contractors, with contact details including emergency numbers in case of an incident

PRE-START MEETING

Organise a pre-start meeting with your installer's project manager as a final check on the planned installation to make sure it meets your expectations and operational requirements and to clear up any differences of opinion. An agenda for that meeting could cover the following points:

- contractor to comply with specific time scales for the project and highlight any long lead times for equipment or specialist labour – for large construction projects phasing of your system installation must be considered in liaison with the main contractor on the site
- confirm risk and methods statements are acceptable and meet your expectations, as these may require work on your system planned around an operational business or a main contractor where additional consideration may be required
- consider working hours, potential noise, staff members and or other contractors
- agree a method of communication for variations/alterations which deviate from the original scheme, as any misunderstandings could have a major impact on the operation of your completed system
- agree regular meeting dates to review progress and discuss any issues that have or are likely to have on the project once started

MANAGING THE IMPLEMENTATION PROCESS

- ensure that review meetings are held in line with the agreed dates – record any delays and issues, and any variations you agree to resolve them
- review the completed system with the installer to ensure that it meets your operational requirements and complies with their quotation and your order (including any agreed variations)
- ensure the system is fully commissioned, including that 'as fitted' manuals and any ongoing training for you and your team are provided by your installer for future guidance (see **Commissioning and user acceptance**)
- check that details for preventative and re-active maintenance have been included in the documentation (see **Operating your system**)

Commissioning and user acceptance

The separate guidance within Stage 3 of the Surveillance Camera Commissioner's **Passport to Compliance** provides buyers and users of surveillance camera systems with detailed information in relation to system commissioning, user acceptance and system handover.

In summary, the key elements for the buyer to consider for system commissioning are:

- document a user acceptance test procedure (see below) to verify the functions and performance of the system
- note any deviations from what was set out in the technical requirement
- test the operation of the system, including each camera, controls and image quality
- test the security of the system, including the provision of passwords and staff training
- record and export images from each camera for future reference

The user acceptance test should be conducted during the operation period and based on both a live or on-screen view and a separate review of recorded images. Establish the following key results:

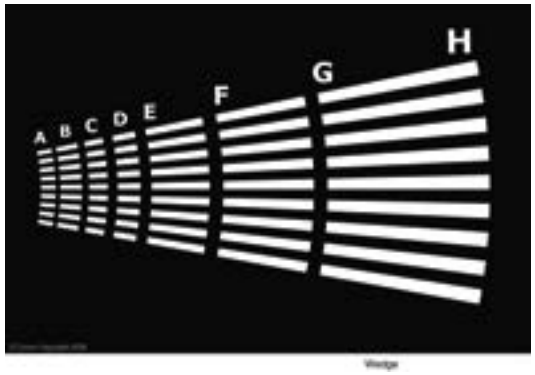
- Is the frame rate suitable for the activity being monitored?
- Does the picture quality from each camera correspond to the different levels of purpose you set in your operational requirement **(identify, recognise, observe, detect)**?
- Is picture quality from any camera affected by reduced lighting at night-time?
- Are recorded images capable of being exported from the system in a simple process?
- Are recorded images of the same quality of those observed during the live or on-screen view?

The **Passport to Compliance Stage 3 download** also includes a checklist for system handover which you may find helpful.

Image Quality Testing

The installer should perform testing of your system using an image quality commissioning test and demonstrate that the system meets your specified requirement. Alternatively you could test the system yourself to ensure that it meets your expectations.

Test targets including these two examples are available for this purpose.



Operating your system

Principle 10 of the Surveillance Camera Code of Practice says:

> *"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."*

It is good practice to review the continued use of your system on a regular basis, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose. This is likely to include both monitoring its performance to see if it remains fit for purpose, and an audit which reviews policies and procedures and whether a surveillance camera system is still necessary as part of the solution to your problem.

Maintenance of your surveillance camera system is important and reference should be made to paragraph 3.4 of the **Passport to Compliance** for a description of maintenance agreements that should be considered.

Similarly, following handover of your system, you should monitor it regularly to ensure it continues to perform as required. Consider setting a schedule for this and conduct a periodic 'walk around' each camera location so that you can identify any environmental factors that may begin to affect the field of view (overhanging branches, shrubbery, etc). Also check that your privacy notices remain visible.

Plans must be developed to maintain security over the lifetime of surveillance camera systems. There must be an active programme in place to identify and assess both cyber and human vulnerabilities and to mitigate these risks in a proportionate manner. This must include being able to safely and securely update software and firmware.

It is also important to conduct audits of your system to check if your surveillance can still be justified, and to verify that all related policies and procedures have been implemented and are being followed. This should include revisiting your DPIA, checking that any privacy zones on cameras remain effective, and checking that the retention period for recorded images is being observed with a full audit trail maintained where any images have been disclosed.

Consider completing the **surveillance camera self-assessment tool** and any action plan that results. You may also wish to consider seeking **certification against the Surveillance Camera Code of Practice**.

Jargon busting glossary

As a non-expert, you won't want to feel baffled by jargon about video surveillance systems. This jargon busting glossary contains many of the technical terms you may hear. It is not intended to include every single possibility, yet should cover most of what you need. For anything else, either challenge the person using jargon or do a quick online search.

CONTENTS

ADSL

ADSL (asymmetric digital subscriber line), commonly referred to as broadband, is a very common method in the UK for connection to the internet over the telephone cable infrastructure.

AUTO IRIS

Security cameras with auto iris have the ability to compensate for large variations in light levels. This is useful for security cameras that need to adjust for changes from bright sunlight to darkness or night. Auto iris circuitry is normally linked to a motorised drive that opens and shuts the iris on the camera lens.

ALARM INPUT

Some DVRs and security cameras have alarm inputs, which can accept connection from a sensor device such as a door contact or a passive infra-red motion detection which trigger the camera or DVR/NVR to take some action such as to begin recording.

APERTURE

Aperture is the hole or opening within camera lens which determines the amount of light entering the camera, the size of which is controlled by the iris and is measured in F numbers. Generally, the lower the F number, the larger the aperture is and consequently more light can pass through the lens.

BACK LIGHT COMPENSATION

This is a feature of security cameras that automatically adjusts the image to compensate for bright light to give more detail on the darker areas of the image. For example, use is to focus on the detail of a face of a person that has the sunlight shining from behind.

BALUN

A video balun enables the transmission of video using unshielded twisted pair (UTP) wire instead of coaxial cable. The word ‘balun’ comes from combining the terms balanced and unbalanced. The function of a balun is to transform an unbalanced signal into a balanced signal. When video signal is transmitted through coaxial cable, the distance travelled by the signal is limited because the signal is in the form of an unbalanced signal that is susceptible to radio frequency interference or noise. Coax cable incorporates special shielding to minimize noise. Video baluns transform the video signal into a balanced form in which each wire in the twisted pair transmits an identical signal with opposite polarized magnetic fields. Noise affects each signal equally. When the signals are combined, the noise is cancelled out. By using a designed balun, an unshielded twisted pair wire can transmit video for much longer distances than coax cable.

BNC CONNECTOR

BNC (Bayonet Neill–Concelman) is a connector for coaxial cable that is most commonly used for surveillance camera system installations.

CCTV

Closed circuit television, generalised term applied to all camera systems but strictly refers to the end to end single cable transmission method from camera to recorder or monitor. The term CCTV is in wide use, but does not really reflect current surveillance camera technology. Industry standards often use the term video surveillance system (VSS) in preference to CCTV. In this guide, we have used the term surveillance camera system (or “system” for short). A surveillance camera system includes the cameras and all the related hardware and software for transmitting, processing and storing the data which is captured.

CCD

Charge Coupled Device, one of the two main types of image sensors used in security cameras. When a video is recorded, the CCD is struck by light coming through the camera's lens. Each of the thousands or millions of tiny pixels that make up the CCD converts this light into electrons. The number of electrons, usually described as the pixel's accumulated charge, is measured and then converted to a digital value. This last step occurs outside the CCD, in a camera component called an analogue-to-digital converter.

C MOUNT LENS AND CS MOUNT LENS

There were 2 main types of lenses used in security cameras. The C mount lens has a flange back distance of 17.5mm. The CS mount lens has a flange back distance of 12.5mm. C mount lenses therefore have a longer focal distance. CS mount became widely used, because it its more practical for many of today's more compact cameras. Lenses are often supplied with a 5mm spacer ring (sometimes called a C ring) that allows a C mount lens to be used on a CS camera. Most modern security cameras nowadays are CS mount.

CO-AXIAL CABLE

A type of cable typically used in surveillance camera system installations that has a central conductor, surrounded by a shield sharing the same axis. The shield can be made from a variety of materials including, braided copper, or lapped foil. There are various standards for specific types of co-axial cable. The cable used for normal surveillance camera system installations has the specification called RG59.

COMPOSITE VIDEO

The encoded output of a surveillance camera whereby the red, green, and blue video signals are combined with the synchronizing, blanking, and colour burst signals and are transmitted simultaneously down one (usually coax) cable.

COMPRESSION

Digital video pictures can be compressed with a number of techniques. There are many varied compressions codecs. These include the more common ones such as JPEG and JPEG-2000 (for still images), M-JPEG and MPEG, H.264, H.265 (for moving pictures).

DVR

DVR (digital video recorder) is a generic term for a device that records television data (see PAL/NTSC) in digital format on a hard drive as opposed to historically recording onto a magnetic tape (commonly referred to as a video cassette recorder VCR). A DVR has minimum functionality of being able to view the recording, playback, fast forwarding, rewinding, and pause the footage.

FOCAL LENGTH

The focal length is the distance between the centre of a lens, or its secondary principal point and the imaging sensor. Lower lengths give a greater field of view and less magnification. Longer lengths give a narrower field of view and greater magnification.

GAMMA CORRECTION

Gamma correction controls and adjusts the overall brightness of an image for consistency.

IMPEDANCE

The total opposition offered by a device to the flow of an alternating current, measured in Ohms.

INFRARED (IR)

Low frequency light below the visible spectrum. Infrared is used in surveillance cameras to provide a light source to record images in dark and zero light conditions.

INGRESS PROTECTION

IP waterproof ratings are a BSI standard measurement for how waterproof something is. Many security cameras or camera housings are designed for outdoor use need to be waterproof, for example IP66 and IP68. The first digit defines the protection against ingress of foreign objects: 0 is the lowest rating and means non-protected; 6 is the highest rating and are used to denote dust tight. The second number defines the level of protection against ingress of water: 0 is the lowest rating means non-protected; 8 is the highest rating and means protects against continuous immersion in water.

INTERNET PROTOCOL (IP)

Set of rules governing the format of data and routing of that data over the Internet or other network.

IRIS

The mechanical device, built into a lens that adjusts to vary the amount of light passing through to the light sensor (CCD chip) of a camera. Also see auto iris, which is more common in modern cameras.

JPEG

JPEG is one of the standards for the encoding and compression of images. JPEG is used in the video surveillance systems to compress and store individual frames of video. JPEG was developed by the Joint Photographic Experts Group.

LCD

LCD (Liquid Crystal Display) is a technology used for flat screen displays.

LED

LED (light emitting diode) is a more modern and lower power consumption technology used in flat screen displays.

LUX

Lux is the measurement of a unit of light luminance, used as a measure of low-light viewing/recording capacity in security cameras. The lower the Lux rating of a camera, the better it will see in low light.

MPEG

MPEG is one of the standards for the encoding and compression of images. The Motion Picture Experts Group (MPEG) released MPEG-4 encoding in 1998. The basic idea behind MPEG is that compressed images are compared before being transmitted over the network. The first compressed image is used as a reference and compared to the images that follow it in the video sequence. The first image is transmitted over the network along with the parts of the following images that differ from the initial reference image. The viewing application on the receiving end of the transmission then reconstructs all images based on this information and displays the result. This is a simplified description of how MPEG-4 works.

NETWORK CAMERA

This refers to a camera that is designed to record pictures and transmit them directly over a computer network or internet connection. The images are encoded directly in one of the standard compression techniques.

NTSC

NTSC (also see PAL) is an abbreviation for the National Television Standards Committee. The term 'NTSC video' refers to the video standard defined by the committee, which has a specifically limited colour gamut, is interlaced, and is approximately 720 x 480 pixels and 30 frames per second (fps). This standard is used in North America/Japan.

This has largely been superseded by digital signal measurement methods.

NVR

An NVR (Network Video Recorder) is a generic term for a device that records data from IP cameras or analogue encoders in digital format on to a hard drive. An NVR has minimum functionality of being able to view the recording, playback, fast forwarding, rewinding, and pause the footage.

OSD

OSD (on screen display) is a method of displaying set-up information such as time and date and/or instructions on a display monitor or directly onto a video stream.

PAL

PAL (also see NTSC) is an abbreviation for Phase Alternating Line. This is the television display standard that is used mainly in Europe, China, Malaysia, Australia, New Zealand, the Middle East, parts of Africa, and other parts of the world. PAL uses 625 lines per frame and a frame rate of 25 frames per second (fps).

This has largely been superseded by digital signal measurement methods

PTZ

PTZ (pan, tilt, and zoom) is the remote control of a camera with real time command over its directional movement and focus.

POE

PoE (power over ethernet) is a method of supplying power to the cameras from the network hardware within the same cable as the video signal (usually Cat5 or 6 Ethernet cable) without the need for an external power source local to the camera.

ROUTER

A device that forwards data packets along IP networks, typically when referred to in surveillance camera system installations. A router is used to connect multiple network devices such as camera, NVR, DVR, network switches etc. to a single internet connection (for example ADSL).

PIXEL

A pixel refers to an individual area on the surface of the imaging device, normally a CCD. It is made from photosensitive material which converts light into electrical energy. In the context of a display monitor, a pixel is also referred to as an individual area on the surface of the screen which converts electrical energy to visible light.

RS-232

RS-232 is a communications standard for serial communications between devices. The RS-232 standard allows for the connection of 2 devices through a serial link, and is an old style protocol used for serial connections in computers.

RS-485

RS485, also referred to as EIA-485, is a communications standard for serial communication between devices. When talking about surveillance systems, RS-485 is typically used as the protocol to allow computers and remote controllers to control the movement of PTZ cameras. RS-485 allows for serial connections between more than 2 devices on a 'daisy chain' network system.

SIGNAL TO NOISE RATIO (S/N RATIO)

This is the ratio between the signal strength and the noise levels on an audio or video signal.

TELEVISION LINES (TVL)

This is a measurement of the (older) analogue resolution of a video device. The higher the number, the higher the resolution is.

VARIFOCAL

This refers to a type of lens that has the capability to change the focal length either manually or electronically (remotely). This allows adjustment of the magnification and field of view of the security camera. Often referred to by the minimum and maximum focal lengths of a lens, for example 2.8mm to 12mm is a common variant.

VIDEO ANALYTICS

Video analytics is usually a separate software or hardware platform which will analyse the video stream and determine the scene. Depending on the complexity (and usually cost) almost any scenario can be recognised and appropriate responses can be activated, for example facial, person, vehicle recognition, and object removed or left, advanced motion detection.

VCA

VCA (video content analysis) is a lower cost variation of video analytics and is a method of using the camera's built in video processing to determine certain criteria (often including 'area detection' or 'cross line detection'), usually with the ability to change the recording quality, frame rate or resolution etc. or to trigger outputs such as external lighting.

WDR

WDR (wide dynamic range) can be either digital (software controlled), or 'true' (optical) alternatives (with differing cost associations). It is a feature which included in some cameras enabling automatic compensation for very dark and very light areas of a scene, so is able to capture clear images of objects surrounded by a strong back light, while still keeping the background visible, for example a camera mounted internally (low lighting) but the scene encompasses the outside (bright daylight), such as a shop door where a person entering can appear silhouetted without the use of WDR.