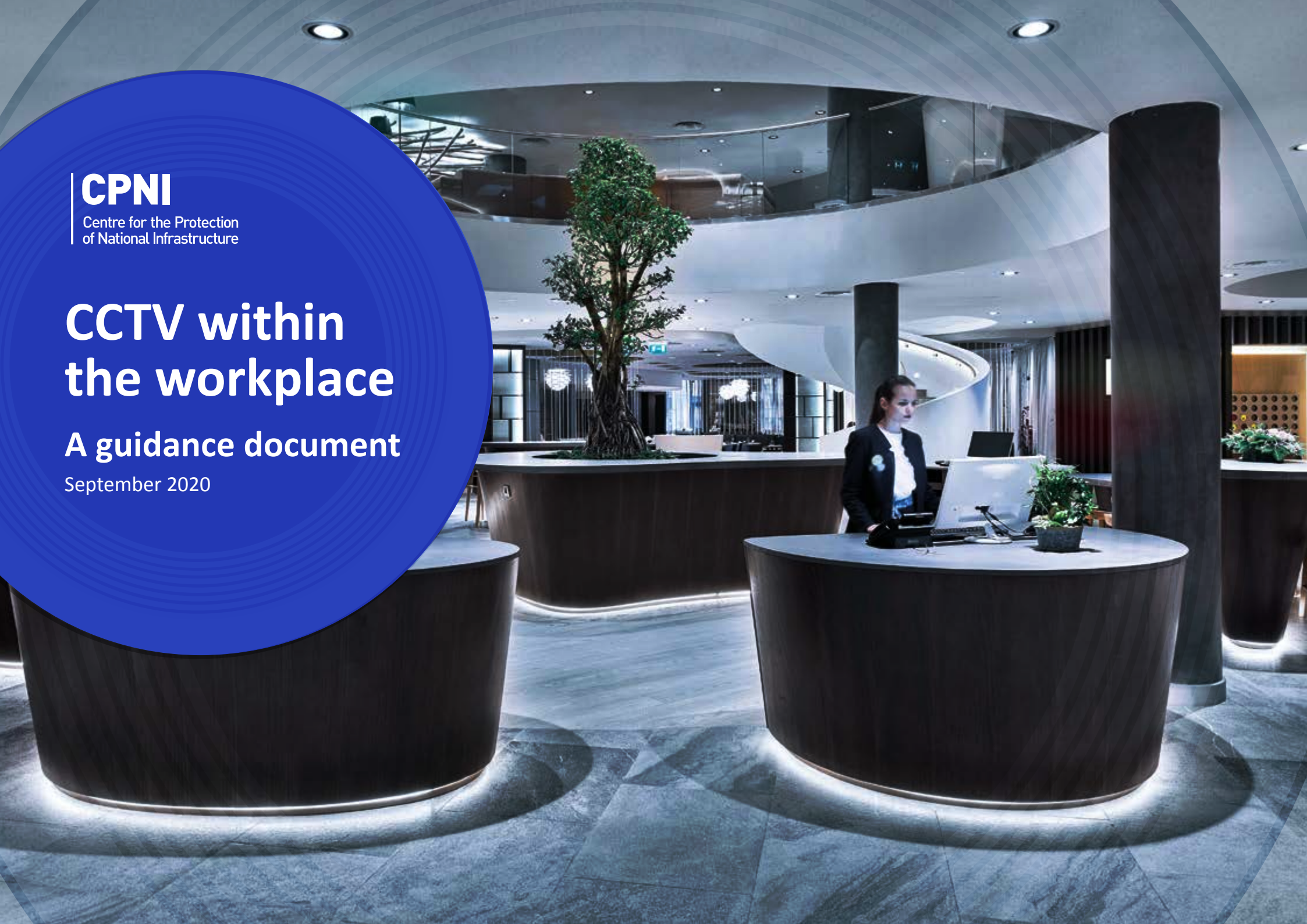


CPNI
Centre for the Protection of National Infrastructure

CCTV within the workplace

A guidance document

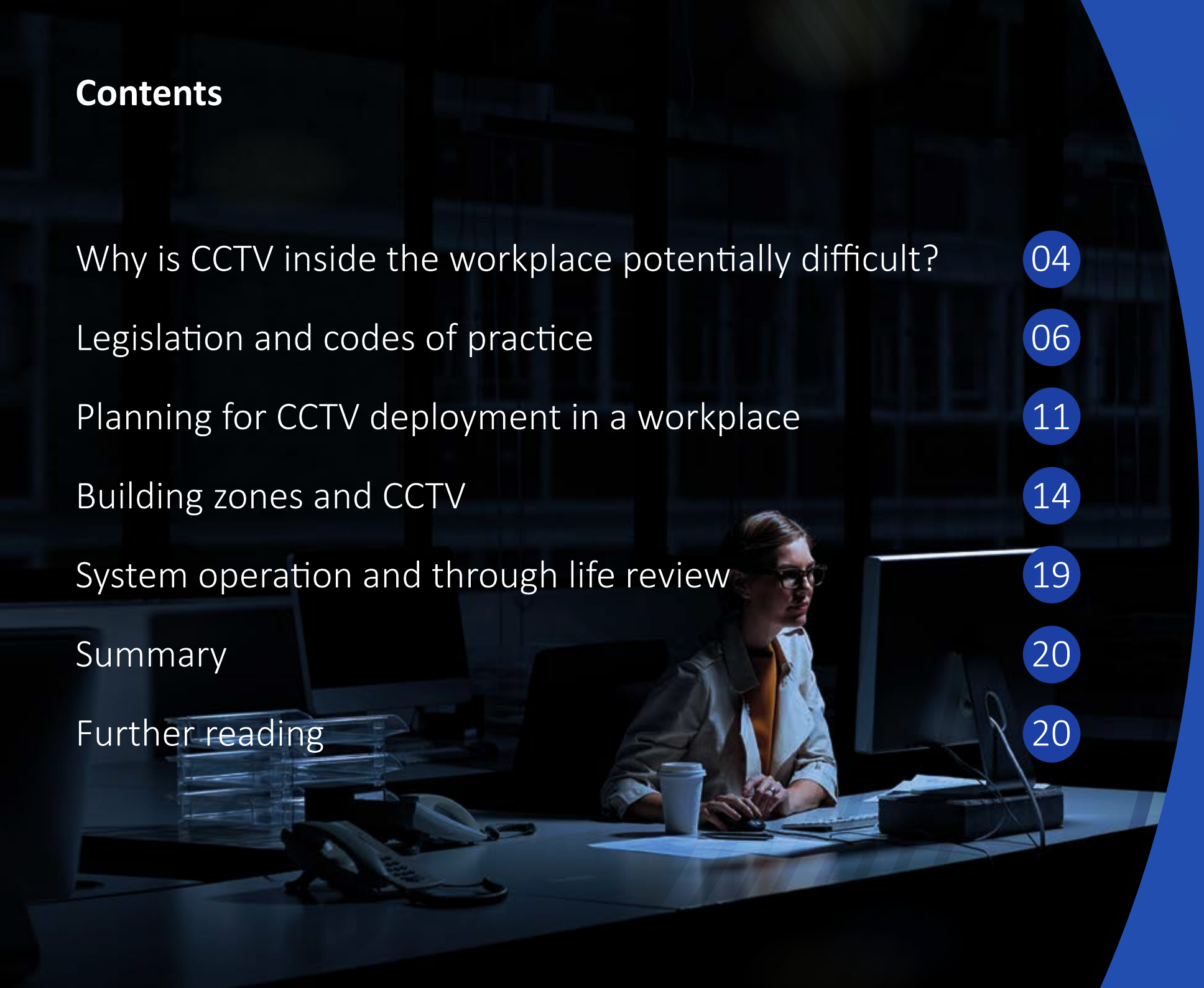
September 2020

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

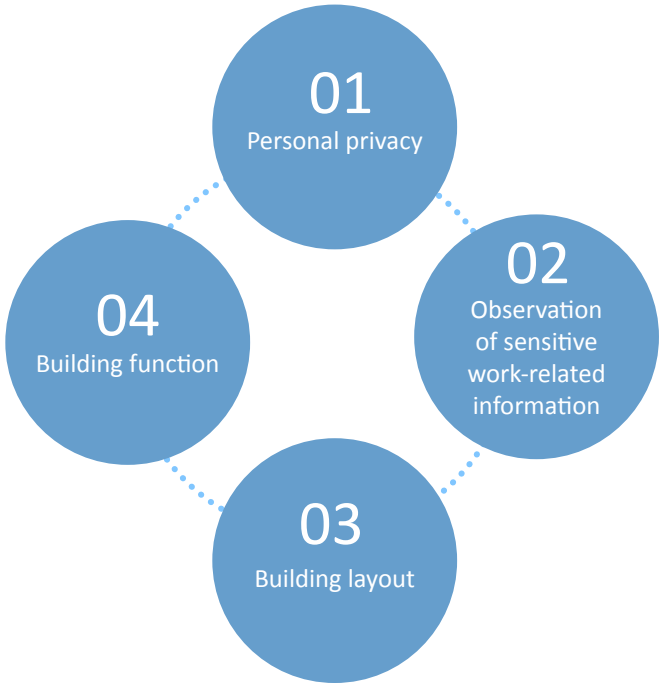
To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Contents



Why is CCTV inside the workplace potentially difficult?

There may be many business drivers leading to a desire to install CCTV within places of work, with two of the most common being safety and security. While the business drivers may be valid, it is important to realise that there are a number of potential issues associated with CCTV installation inside the workplace, such as:



This guidance is focussed on issues surrounding the implementation of CCTV within the workplace for security purposes, but also mentions where there might be strong drivers for other types of requirement.

As with any CCTV installation, remember that it is a legal requirement to ensure that the purpose of any CCTV within the workplace is clearly defined and documented.

It is unlikely that those monitoring CCTV have a requirement to know sensitive information. Who has access to the images?

Personal privacy

Employees may be allowed to undertake some personal activities on corporate IT, such as checking personal email accounts or non-work related websites. They have a right to privacy while undertaking these activities, which should be in accordance with corporate 'Acceptable Use' policies and other conditions of employment.

Sensitive work-related information

Most information used in the course of work is likely to have a degree of sensitivity for your business for one or more of the following reasons:

- Commercial interests, e.g. pricing models
- Business operations, affordability
- Business security, e.g. operational plans and procedures
- National security where information is subject to the Government Protective Marking Scheme

In all cases it is safest to assume that the information is being worked upon on a 'Need to know, right to know' basis. It is highly unlikely that those responsible for monitoring the CCTV system will have either the right or the need.

Building function

Buildings support many different types of operations and workplaces that have different levels of inherent risk for individuals and the business. Understanding all activities and where they occur should form a key part of the requirements definition process. Examples of the range of activities are desk-based work, distribution centres and workshops.

Buildings may also have a mix of semi-public and private areas (e.g. a reception area) or be wholly private with access control on the perimeter of the building.

Building layout

The layout of a building can have a big impact on both the affordability of CCTV and its potential to affect large numbers of people. To provide area coverage, open plan areas are likely to require fewer CCTV units than traditional small office layouts; but, as a result, each camera will be able to see the activities of more people.

Legislation and codes of practice

Surveillance systems have the potential to intrude to a significant degree on people's privacy. This potential increases as systems become more complex and automated. Legislation and codes of practice have been developed to try and strike the correct balance between the rights of the individual and those of system operators.

Data Protection Act

The Data Protection Act defines the law on processing and holding data on identifiable living people.

Human Rights Act

The Human Rights Act adopts the rights contained in the European Convention on Human Rights into UK law.

Information Commissioner's Office (ICO) Code of Practice

This code of practice explains the requirements for operators of surveillance systems to meet in order to be compliant with the Data Protection Act. It also offers strategies to mitigate any negative social impact from increasingly sophisticated surveillance systems.

Surveillance Camera Code of Practice (Home Office pursuant to the Protection of Freedoms Act 2012)

This code of practice was issued by the Home Secretary to reinforce individuals' confidence that surveillance cameras are deployed to protect and support them, rather than to spy on them. It has been developed with a focus on CCTV deployed in public spaces, but has wider applicability.

It should be noted that codes of practice are not mandatory, but following them is considered to be best practice.

When thinking about Data Protection, a good starting point is the eight data protection principles.

Data Protection Act

The Data Protection Act, also known as the DPA, provides legislation relating to the following issues:

- Processing personal data fairly
- Obtaining personal data lawfully
- Accuracy of personal data
- Storing personal data for appropriate periods of time

Complying with the Data Protection Act

It is important to ensure that the requirements for, and implementation of, any system will be compliant with the legislation defined in the DPA. Otherwise, you could be taken to court by those under surveillance.

A good place to start would be to review the eight data protection principles that are defined in the Act. They can be applied in various contexts and help to ensure that information is processed lawfully.
See overleaf.

The eight data protection principles

01

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

02

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

03

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

04

Personal data shall be accurate and where necessary, kept up to date.

05

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

06

Personal data shall be processed in accordance with the rights of data subjects under this Act.

07

Appropriate technical and organisational measure shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of destruction of, or damage to, personal data.

08

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Article 8 of the ECHR and HRA provides legislation for the respect for an individual's private and family life, home and correspondence. This legislation must be adhered to by all public authorities.

Human Rights Act

Though the issues covered in this legislation are wide ranging, including elements such as freedom of thought and prohibition of torture, the most pertinent to surveillance systems is the issue of privacy.

Article 8 of the ECHR and HRA provides legislation for the respect for an individual's private and family life, home and correspondence. This legislation must be adhered to by all public authorities. Given this, surveillance should not be used in any way that might impact upon an individual's privacy.

Even if you are not representing a public authority or undertaking a public function, Article 8 of the HRA may be considered a measure of good practice.

Information Commissioner's Office Code of Practice

The Information Commissioner's Office, ICO, Code of Practice provides an important 'translation' of the requirements contained in the Data Protection Act into strategies to assist.

The ICO Code of Practice offers strategies on the following issues:

- Deciding when surveillance systems should be used
- Data retention and disposal
- Freedom of information obligations and requests from individuals to see the data held about them
- Selecting an appropriate surveillance system
- Maintaining quality control
- Transparency responsibilities

Home Office Surveillance Camera Code of Practice

The Surveillance Camera Code of Practice provides guidance on the following issues:

- Justification for surveillance systems
- Understanding privacy
- Understanding transparency
- Responsibility and accountability
- Outlining rules, policies and procedures
- Storing recorded information
- Restricting access to recorded information
- Maintaining accurate and relevant information

It sets out the following series of 'Guiding Principles' to be followed when defining, implementing and operating CCTV systems:

Whilst the Surveillance Camera Code of Practice is largely written to cover surveillance systems watching public spaces, all operators and users of CCTV systems in England and Wales are encouraged to adopt it voluntarily as a measure of good practice.

01 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.

02 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

03 There must be as much transparency in the use of a surveillance camera system as possible, including a published contract point for access to information and complaints.

04 There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

05 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.

06 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.

07 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.

08 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.

09 Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10 There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are compiled with in practice, and regular reports should be published.

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.

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.

Planning for CCTV deployment in a workplace:

Overview

Given the potential sensitivities associated with the deployment of CCTV inside workspaces, it is very important to ensure that you follow a rigorous, structured methodology for determining and capturing the system requirements.

This process should be seeking to achieve:

01 A documented set of requirements, with an audit trail to explain how the solution has been arrived at

02 Confirmation that the proposals will be compliant with relevant legislation and codes of practice, and an outline of how this will be ensured/enforced throughout the life of the system

03 Stakeholder agreement that the proposals are proportionate to, and a good way to deal with, the issue(s) faced

04 An understanding of organisational readiness issues to be addressed prior to implementation

Requirements development

A structured requirements development process should always be carried out whenever new security measures are to be installed. It is especially important to do this for potentially contentious systems such as internal CCTV. It is also important that key stakeholders are asked to sign-off requirements at key stages in the process to provide an audit trail and record of consultation and agreement.

As part of the risk assessment process, you should consider whether the risks are related to specific, short-term needs (e.g. to investigate an isolated problem). If this is the case, it is likely that internal CCTV might not be a cost-effective or proportionate solution.

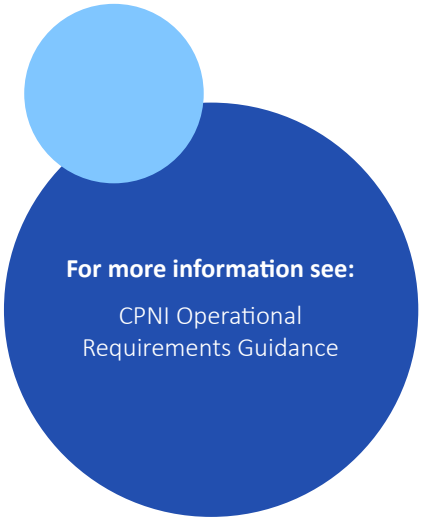
The risk assessment should include relevant non-security-related risks (e.g. safety in a hazardous operating environment) in order to build a comprehensive picture of why CCTV within the workplace is being considered.

It is important to obtain stakeholder agreement of the risks. Then you should consider the most appropriate means of mitigating these risks. For workplace risks it is recommended that non-CCTV solutions should be given priority, with CCTV being considered as a solution of last resort.

As an example, it might be determined that implementation of a better security culture, or effective enforcement of the existing one, would mitigate the risks to an acceptable level without the need for CCTV. Another example might be the use of appropriate motion detection sensors.

If the process results in stakeholder agreement that internal CCTV is a valid part of any solution, the requirements process should seek to document the following:

- The rationale and reasons behind the necessity for CCTV, preferably stating why these cannot be effectively achieved by other means.
- User requirements for the system such as what the cameras are seeking to achieve and how the system will be operated. This should look at the different functional areas within the building and the requirements should be unambiguously stated in language that can be understood by non-specialists.
- Constraints for the coverage, e.g. what will the system be excluded from monitoring. It is also useful to think about how this may be demonstrated/proved to concerned individuals.
- Recording and playback requirements, including but not limited to: what will be recorded and why it is being recorded; how recorded footage will be protected; who will be able to access recorded information; how long recorded footage will be retained and how it will be securely erased; people's rights to access information held about them.
- Whether existing CCTV control facilities / control rooms have capacity to support the additional CCTV.
- How ready is the organisation for implementation of such a system.
- Supporting requirements such as signage.



Stakeholders

Engagement with stakeholders should form a standard part of the process for determining requirements for any security related systems. This is especially important when considering sensitive issues such as the potential deployment of CCTV within a workspace.

There may be additional groups of stakeholders, such as workers representatives, who don't usually need to be consulted about developing security requirements. However, they should be consulted for any proposed CCTV within the workplace.

Stakeholders should be involved at an early stage of defining the requirements and then engaged regularly for input and feedback as the requirements develop.

Once a system has been implemented, you should consider including all stakeholders in routine through life reviews to confirm that the system can still be justified and is still delivering the required result.

Organisational readiness

Before agreeing to any installation and commissioning programme, it is important that the wider business is ready for the new system.

In addition to training for system operators and administrators, there may be requirements to:

- Revise terms and conditions of employment
- Produce new policies and procedures for staff and operators, potentially including a process for requesting information related to an individual
- Temporarily relocate staff or equipment during installation and commissioning works
- Vet potential contractors
- Implement appropriate messaging programmes to explain to staff what is happening and why

Engagement with stakeholders should form a standard part of the process for determining requirements for any security related systems.

Building zones and CCTV

Overview

While buildings will differ in both layout and function, they will tend to have one or more of the following types of spaces within them:

- Semi-public areas
- Workspaces
- Secure/sensitive areas
- Transit areas
- Rest rooms / breakout areas

The requirements for CCTV in each of these areas will vary, as will the likely ease of justifying why CCTV is being installed.

Workspaces

Workspaces is a broad definition of areas that can vary widely in both form and function. Offices with desks, warehouses, workshops and laboratories are all examples of workspaces. The drivers and justification for CCTV in these areas are likely to differ depending on the nature of the work being undertaken.

It is also worth noting that workspaces generally sit behind access control lines, reception areas etc. and that the desired effect might be achieved through deployment of CCTV in these areas.

During the requirements capture process it is recommended that non-CCTV methods of mitigating risk to an acceptable level are considered first, with CCTV only being considered as a last resort.

Hazardous environments such as warehouses or workshops may justify the installation of CCTV. In fairly benign environments, such as offices where desk-based work is conducted, installation would be less justified.

Surveillance in hazardous workspaces might be used to:

01 Monitor health and safety hazards

02 Enforce safe working practices

03 Potentially help to limit access to appropriately trained and authorised personnel, although this could be achieved by placing CCTV at the entrances to the area, rather than within the workspace itself

Surveillance in office environments is unlikely to be justifiable and proportionate in most cases, although this assertion should be tested during the development of the requirements. It might be suggested that CCTV could be used to investigate employee misconduct; however, this is unlikely to be proportionate to the risks faced. If the need is believed to be genuine, then a rigorous requirements capture process, engaging with all relevant stakeholders, must be undertaken.

There may also be workspaces where it is vital that the correct procedure has been followed, for example at a laboratory processing evidence. Appropriate CCTV footage might form part of the proof that process was duly applied, but this would need to be balanced against the rights to privacy of the workers in the laboratory.

Potential issues

There is a high degree of sensitivity associated with the deployment of CCTV within a workspace. Justifications for requirements in such areas should be comprehensive and must take account of intrusion and privacy concerns. They must also pay particular attention to the legislation and codes of practice.

CCTV might capture images of sensitive material being worked on, either on screen or paper.

Deployment of CCTV within a workplace may well require considerable organisational readiness issues to be addressed, such as potential impacts on terms and conditions of employment.

If investigating employee misconduct is a significant concern, it is important to acknowledge the alternative, less invasive methods that are available. For example, with more stringent employee vetting, as well as specialist software, the need for surveillance as a means of investigation of misconduct might be mitigated.

Semi-public areas

Within this guidance, a semi-public area is defined as any area in the building where non-vetted individuals, such as visitors and clients, can congregate before being met by their host or provided with an access control token. If a building is multi-occupancy there may well be a building reception and then a separate reception for each tenant.

Depending on the nature of the site, visitors may have had to undergo initial vetting at the perimeter, but public areas are typically easily accessible with unrestricted access. Therefore, reasonable justification is needed for comprehensive CCTV coverage in these locations.

Surveillance in semi-public areas might be used to:

- Deter unwanted individuals from entering the building, although this might well be achieved more effectively through the use of perimeter CCTV
- Identify unwanted individuals that enter the building
- Detect hostile reconnaissance
- Deter unwanted behaviour
- Identify unattended objects
- Monitor the main access control line (i.e. turnstiles) for both entry and exit activity
- Monitor potential health and safety hazards

It is worth noting that some semi-public areas may also include areas where people can come to have meetings, avoiding the need to take visitors into the secure areas of the building. If these are open plan within the reception area, then they will fall under the guidance above. If they are closed-off areas, then placing CCTV is not recommended.

Potential issues and opportunities

Surveillance in semi-public areas is unlikely to raise many issues, however it is important to think carefully about the implications of surveillance.

If there is an opportunity to assess layouts of existing reception areas, it is worth considering alternative, more effective deterrents than CCTV. Examples of these could be maximising lines of sight or placing reception desks that everyone entering the building must go past.

For all secure/sensitive areas, the use of CCTV to reinforce access control may well be a reasonable requirement.

Secure/sensitive areas

Secure and/or sensitive are areas might be present within a building for a variety of reasons, including:

- To store controlled substances such as chemicals
- To hold IT servers or other equipment critical to the operation of the building
- To hold sensitive information, e.g. an archive
- The area being the location where board level corporate activity takes place
- Armouries
- Security control rooms
- Cash handling rooms

The areas are likely to have strict access control, limited to only a few authorised personnel, and any work on the area is likely to be governed by mandatory processes and procedures.

The extent of any potential security requirements will depend on the nature of the area being protected.

For all secure/sensitive areas, the use of CCTV to reinforce access control or capture images of people entering/leaving the area may well be a reasonable requirement.

Deployment of CCTV within a sensitive or secure area is likely to depend on the activity taking place.

Areas where work is normally intermittent and subject to some kind of permit to work system (such as equipment rooms and chemical stores) may benefit from internal CCTV coverage. This would confirm that only the expected activity is taking place or assist in responding appropriately if unexpected activity is taking place. The requirements process should consider the type of coverage needed to most effectively assist with protection of the asset and supporting response teams.

If the area is a location where sensitive activity occurs on a continuous basis (such as board level offices and security control rooms), the justification for CCTV coverage will be unlikely.

Specific coverage for specialist areas such as cash handling rooms is likely to be justifiable on the grounds of asset protection.

Potential issues

The use of CCTV to monitor entry and exit points from secure/sensitive areas is unlikely to present any major issues with regard to justification. This applies as long as the CCTV is appropriately focussed on the entry/exit points rather than any surrounding workplaces.

Requirements for CCTV coverage within a sensitive or secure area may well be contentious depending on who has access, but this should be balanced against the need to protect business operations.

Transit areas

Transit areas, such as lift lobbies, corridors and stairwells, are used to gain access and move around the building. Most will only have internal access points but some, such as fire escapes, will have external entry points.

The ease with which surveillance may be justified in transit areas will depend on how they are used and who uses them.

If the transit area includes a building entry or exit point, then CCTV could well be installed to capture images of people and activity, focussed on the access point. This can be extended to lift lobbies or stairwell entrances that are just inside the building access control line, particularly if these are not protected through the use of full height security measures such as portals.

Areas that should normally be empty (e.g. a back of house corridor leading to a secure area) might require CCTV to provide situational awareness to security personnel and to support any response to unexpected activity.

For areas such as corridors and lift lobbies within an access-controlled area of a workplace floor plate, security surveillance is harder to justify as a proportionate response to the risks faced. There might be non-security-related reasons for installing CCTV in specific locations, such as an area that has identified health and safety hazards.

Potential issues

Depending on the layout of the floor plate, it might be difficult to limit the area of view of any CCTV so that it will not intrude into areas where work is conducted.

People using transit areas inside a workspace might well be carrying sensitive information, and this could result in CCTV covering these areas inadvertently capturing images of this.

Restrooms/ breakout areas

Rest rooms and breakout areas are both non-work-related areas. Legislation and codes of conduct emphasise the importance of upholding an individual's right to privacy. It would therefore be very difficult to provide adequate justification for any CCTV coverage within these areas.

System operation and through-life review

As part of the requirements definition process for workplace CCTV, stakeholders should have been asked to consider who can operate/access the system.

Thought should also have been given to implementation of regular review processes to confirm that the system is still justified and delivering its aims.

Monitoring and accessing the surveillance system

Whenever a CCTV system is being defined, thought should be given to how it will be controlled/monitored and who will be able to access it. This is particularly important in the case of workplace surveillance or other potentially sensitive CCTV installations.

The requirements definition process should therefore ensure that the following types of issues receive particular focus:

- Will all CCTV operators/supervisors be able to access the in-workplace footage, or should it be limited to those with a higher level of vetting or who have received additional training?
- Does the system require pro-active monitoring or is it only to be used for post-incident investigation?
- Should a dedicated workstation/monitoring area be established to limit unintended observation of the system?
- Additional controls on who can access recordings from workplace CCTV, for instance requiring a more rigorous justification/ authorisation process.
- Integration into the site-wide response models

The last of these points may be quite complex as the answer is likely to vary depending on the nature of the incident being responded to.

Through-life review

Once any system has been installed, and particularly in the case of CCTV in the workplace, it is important that a programme of regular through-life monitoring and assurance is implemented. This will help retain support for the surveillance system.

Among other items, the following should be considered at each review cycle:

- Is the implementation correct and is the desired effect being achieved?
- Is the system being operated correctly?
- Have you appropriately limited who can see live images or recorded footage?
- Do the risks and justifications still exist? Have they changed?
- Has any part of the building changed function?
- Has the nature of the work being undertaken changed?
- Are there any refinements that could be implemented?
- Are information assurance and right to privacy being adequately addressed?

Summary

CCTV in the workplace is a contentious subject. There are many reasons why you might NOT install CCTV inside your buildings. There are, however, many reasons why you would want to install CCTV inside a building. Not least are huge benefits should you have an intruder in the building. The tactical positioning and use of CCTV inside your building will allow your security officers in the Control Room to track the intruder as they make their way around. Even CCTV in stairwells and corridors will provide a huge advantage. Failing that, cameras in stairwells might be considered, so at least the Control Room can identify which floor an intruder is on. In short, any CCTV within the building will be a force multiplier in the case of an incursion and should be considered as such – this in itself might be the basis of your OR.

Further Reading

CPNI CCTV for Perimeter Security
CPNI.GOV.UK

CPNI CCTV Within a Site
CPNI.GOV.UK

Surveillance Camera Code of Practice
GOV.UK

Information Commissioner's Office Code of Practice
ICO.ORG.UK