Office of
Crime Prevention

Western Australia
Closed Circuit Television (CCTV) Guidelines

CONTENTS

1 INTRODUCTION

Owners of CCTV systems should determine their own objectives and risks in order to select and operate an appropriate system to meet their objectives.

The use of CCTV technology has become increasingly popular to address crime reduction and community safety issues. As the popularity of the technology has grown, Western Australia has seen a significant increase in the number of systems being installed and used. The Western Australia State Government has responded to the increased use of CCTV technology by developing the Western Australia State CCTV Strategy. This strategy seeks to achieve "enhanced crime risk management through the effective and responsible use of CCTV within a range of strategies."

These guidelines have been developed as part of the State Government's CCTV Strategy to enhance the capacity of government agencies, local governments, businesses, communities and the public to implement and utilise CCTV in an effective and responsible way. The guidelines have been produced to assist those people or organisations who are considering the implementation of CCTV by highlighting relevant planning and technical factors which should be considered at each step of the CCTV implementation process.

Research into the effectiveness of CCTV as a crime prevention tool in public places has shown mixed results, with some case studies suggesting CCTV has reduced crime levels and others suggesting that no improvement in crime figures resulted or that crime even increased.

In order to maximise the potential benefits of CCTV, careful consideration must be given to a range of factors so that specific objectives for CCTV can be clearly determined for each case, and consideration given to the likely success of CCTV to manage risk prior to implementation. In this respect it is critical that the intended purpose be clear, that the risks are assessed in terms of the known or anticipated threats, and that CCTV be considered in the context of holistic security and crime prevention measures tailored to address the identified threat and risk.

CCTV can be expensive to implement, manage and maintain, and may be ineffective if installed for the wrong purpose or if supporting measures are not put in place. There are also privacy and legal issues that need to be considered. The choice to employ CCTV should not be taken lightly and careful consideration should be given at each step in the implementation process. This will allow for informed decisions to be made about the use of CCTV prior to its implementation.

These guidelines are divided into three sections:

- Introduction to CCTV,
- Background to CCTV,
- Planning and Implementation Process.

The content of these guidelines is based on information current at the time of development (October 2009).

For further reading on the effectiveness of CCTV, a suggested reading list is provided at the end of this document.

These guidelines are not able or intended to provide a means of selecting the right CCTV system for a particular user or application. Owners of CCTV systems should determine their own objectives and risks in order to select and operate an appropriate system to meet their objectives.

The Office of Crime Prevention can not provide legal interpretation of legislation relating to CCTV and content within this guideline should not be viewed as such. The Office of Crime Prevention recommends that organisations employing CCTV should seek legal advice to ensure compliance with West Australian and Australian legislation.

2 INTRODUCTION TO CLOSED CIRCUIT TELEVISION (CCTV) CCTV'S ROLE IN SECURITY

Security comes in many forms, including (but not limited to): locks, fences, barriers, guards, patrols, CCTV, access control, intruder detection, security management and security policies and procedures. With so many possible security measures available it can sometimes be a challenge to determine what specific action should be used to manage risk for a particular application or situation.

Selection of security measures should be based on: clear objectives, minimising loss, cost/benefit, and a formal documented risk management process. It is also beneficial for the individual/s determining security requirements to have experience in managing security risk, a good knowledge of the limitations of security (what it can and cannot do), technical knowledge of security (when required) and criminology theory.

Ideally, security should:

- **Deter** (would-be offenders),
- **Detect** (offenders/incidents),
- **Delay** offenders for a period long enough to
- **Communicate and Respond** to an incident to prevent it occurring or at least minimise loss in the event it has occurred.

All of these roles should be accomplished swiftly and efficiently to provide effective security. The order in which these roles occur is also important.

CCTV as a specific form of security is generally implemented for the purpose of:

- **Detection** – indicating that something is happening in the field of interest;
- **Recognition** – determining exactly what is happening; and
- **Identification** – determining who is involved in the activity.

The degree to which the system will be required to detect, recognise or identify objects in the field of interest will, in part, determine the type of equipment needed and budget required.

When contemplating the implementation of CCTV as a security measure, consider which of these roles of security (Deter, Detect, Delay, Communicate and Respond) CCTV could be achieved. CCTV may deter some types of offenders, but not others. If CCTV is actively watched (or monitored) it may assist in detecting incidents as they occur. Although some advanced CCTV systems generate alarms that can proactively alert security personnel to an incident or allow automatic tracking of suspects as well as other advanced forensic tools, CCTV generally does not assist in delaying offenders or responding to incidents, unless its coverage is sufficient to allow monitoring staff to follow or track a perpetrator until a response force can detain them. This can be expensive in terms of personnel, hardware and intelligent software.

Therefore to achieve effective security, CCTV requires careful consideration and other supporting strategies to facilitate all roles of security. This may include strategies such as: Crime Prevention Through Environmental Design or Designing Out Crime, target hardening, community awareness campaigns, offender diversion, and other crime risk management interventions.

3 BACKGROUND TO CCTV

Strengths and Limitations of CCTV

CCTV has a range of strengths and limitations. In order to use CCTV effectively it is important to understand its capabilities. The following sections outline some of CCTV's strengths and limitations:

CCTV's Strengths

1. Recorded CCTV can be a valuable tool for police when investigating incidents. If a CCTV system can adequately record quality images of an incident or crime, the images may assist police by providing evidence or general information that could assist a subsequent investigation. For example, the colour of clothing an offender was wearing, vehicle make/model etc.
2. CCTV can deter some types of crimes/offenders. If offenders are aware of the presence of CCTV, and the offender perceives that CCTV may increase the likelihood that they will be captured on footage and caught as a result, then CCTV may deter them from offending in the immediate area.
3. Monitored CCTV may be able to assist in identifying incidents. If CCTV is actively watched (or "monitored") monitoring staff may be able to identify incidents and initiate a response to prevent incidents or, more likely, reduce the consequences of the incident occurring. Similarly, some CCTV systems may be able to make use of video analytics to detect some forms of unwanted behaviours.
4. CCTV may assist safety perception. Using cameras in areas may help normal users of the space feel safer and therefore more likely to use the area. More people using the area may increase potential witnesses to potential crimes or unwanted behaviours (potentially deterring offenders), so increased perceived safety may lead to increased actual safety.
5. CCTV works best in areas with good access control. Access control refers to strategies that limit access to areas or an individual's ability to move through a targeted area. For example, swipe card access, doors, hallways, and roads all to some extent limit movement through a targeted area. When movement is limited it becomes easier to predict where individuals or vehicles will be, therefore making it easier to locate cameras to capture images of potential offenders. Access control can make it more difficult for offenders to avoid being captured on footage.
6. CCTV can be a useful tool for police in gathering intelligence. Information recorded by CCTV systems can provide police with valuable intelligence on the types of crimes being committed within an area, how these crimes are being committed and the times that they are likely to occur. This can assist police to plan responses to crime issues within a targeted area.

CCTV's Limitations

1. Cameras can become the target of theft or vandalism. CCTV cameras can be expensive and may be desirable targets of theft. Offenders may intentionally try to damage cameras in an effort to avoid being captured on footage, or opportunistic vandals may throw missiles at cameras simply for amusement. Consideration should be given to the location of cameras to facilitate security of the camera, but also allow the camera to be easily maintained. Additional security may be implemented to provide security for cameras (eg. housings and anti-climb devices). For further information see the section on *Locating and Securing Cameras*.
2. Offenders may avoid the immediate areas in view of CCTV or take measures to hide their identity (eg. by wearing hats or "hoodies"). To provide the most value for evidential purposes, CCTV should provide clear images of an offender's face. Offenders may know this and may take precautions to obscure camera views of their face by wearing hats or hoods.
3. Crime or unwanted behaviours may be displaced by CCTV (eg. to a different location, time, or crime-type). For example, a known hotspot may be identified and subsequently fitted with CCTV, but the offenders/incidents may simply be moved (displaced) to another location. Displacement can occur in different ways. Offenders could move to another location; change the time they offend; change the type

3 BACKGROUND TO CCTV cont'd

of crime they commit or alternate offenders may replace the original ones.

If the intended purpose of CCTV is to deter crime/unwanted behaviour in a particular area because the crime/unwanted behaviour can only occur in that area (eg. CCTV installed in a bank to deter robbing the bank), displacement may be less of an issue.

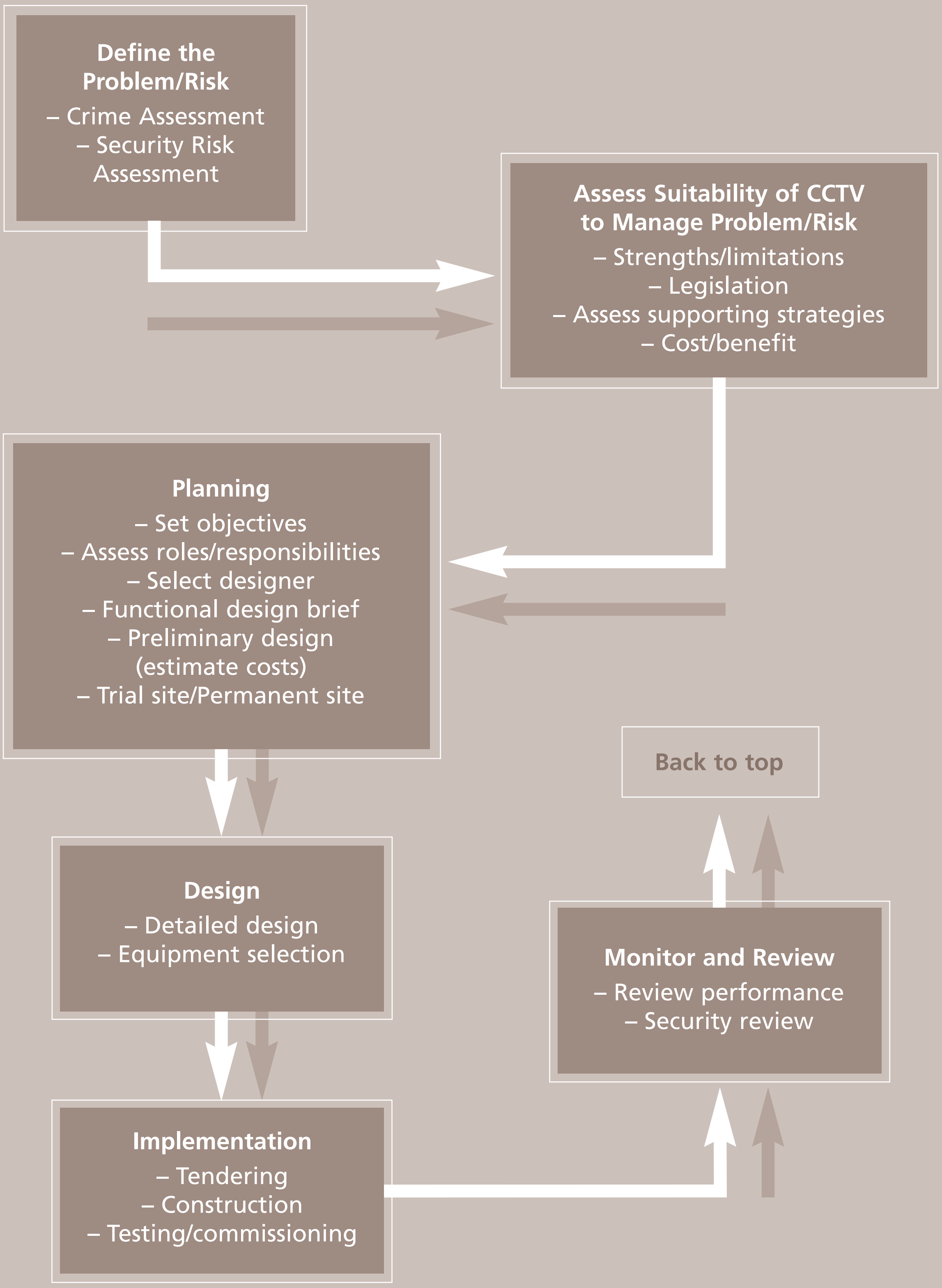
If the intended purpose of CCTV is to deter crime/unwanted behaviour in one area but the same crime/unwanted behaviour is just as likely anywhere (eg. graffiti) displacement can be a challenging issue and may render CCTV ineffective.

CCTV planning should take displacement into consideration to facilitate more effective use of CCTV. This may include utilising telephoto or zoom lenses to provide extended coverage.

4. Offenders may learn or test response times (if CCTV systems are monitored) to avoid apprehension. If CCTV is not monitored (actively watched by monitoring staff) then CCTV is not likely to assist in initiating a response to prevent or manage an incident. If CCTV is monitored, incidents may be noticed as they occur and a response to an incident may be initiated. There is a delay between the time an incident is identified and the arrival of a response capability (eg. guard or police). This is often referred to as the response time. Ideally a response time needs to be swift enough to prevent or manage an incident. If it is not offenders will be able to commit offences and leave the scene before they can be apprehended. Offenders may test how long a response time is before committing offences so they can time their activities to avoid being apprehended.
5. If CCTV is not monitored (actively watched by monitoring staff) then CCTV is not likely to assist in initiating a response to prevent or manage an incident. If there is no immediate response to incidents the deterrent-value of CCTV may be reduced as offenders may realise that they can still offend without being caught, especially if they take measures to disable cameras or hide their identity.
6. If CCTV is to be used for providing information to assist investigation or for use as evidence in court generally, recorded images need to clearly show an offender's face (or similar valuable identifying information) in order to be of value. Many issues can stand in the way of achieving this. These include but are not limited to: poor quality images, insufficient storage time (images may have been erased or recorded-over), offenders may cover their faces, or cameras may be disabled before the offender can be viewed.
7. CCTV may create a false sense of security. People may feel safer if they know, or think that the area they are in is fitted with CCTV. However, if CCTV is not monitored, or if the equipment installed is a false or "dummy" camera, a response to an incident is unlikely to occur. Therefore, an area may actually be no safer if it is seemingly equipped with CCTV and individuals (potentially with a false sense of security) may place themselves at risk unknowingly.
8. CCTV in housings, and CCTV lenses outside housings, can be defeated by paint or other substances so that the cameras lose vision or the vision is seriously impaired. Advanced CCTV systems can generate alarms in the event that cameras are painted or shifted from their designated position.
9. CCTV becomes less effective if incidents take place and perpetrators are not apprehended, because word of the ineffective nature becomes widespread.
10. CCTV relies on good lighting levels to obtain clear and accurate vision. Over illumination, such as facing into the sun or artificial light directed into the camera lens, may reduce the level of efficiency.
11. The 'field of view' may be limited by certain camera types and positioning, creating blind-spots or the absence of surveillance within an area.
12. CCTV is ineffective during losses of power, unless it is connected to an uninterruptible power supply (UPS).

4 PLANNING AND IMPLEMENTATION PROCESS

KEY STEPS FOR CCTV



Define the Problem/Risk
– Crime Assessment
– Security Risk Assessment

Assess Suitability of CCTV to Manage Problem/Risk
– Strengths/limitations
– Legislation
– Assess supporting strategies
– Cost/benefit

Planning
– Set objectives
– Assess roles/responsibilities
– Select designer
– Functional design brief
– Preliminary design (estimate costs)
– Trial site/Permanent site

Design
– Detailed design
– Equipment selection

Implementation
– Tendering
– Construction
– Testing/commissioning

Monitor and Review
– Review performance
– Security review

Back to top

General Considerations

If CCTV is being considered for crime prevention, some very fundamental questions should be asked, including:

- Do we really need it?
- Why do we need it?
- What are its objectives?
- What issues will it assist in managing?
- Will it manage these issues effectively?
- Will other strategies manage these issues more cost effectively than CCTV?
- Do we have existing measures and personnel to support CCTV?

Crime and risk assessments assist a determination of whether CCTV is likely to be effective against certain types of crime in particular applications.

The following sections outline further general information that should be considered at the outset if CCTV is being considered as a crime management tool.

Step 1 – Define the Problem and Risk

Do You Need CCTV?

Risk Assessment

Before specific security measures of any sort are considered, an assessment of the threat and risk should be undertaken to determine the nature of the problem and the desired outcomes. For example, if the threat is *muggings in the street* and the desired outcome is prevention rather than *post-hoc identification* of the perpetrators, CCTV may not be an ideal solution unless it is monitored actively and a response force is rapidly available, which may not always be possible.

The risk assessment will, if undertaken properly, identify security measures likely to address and mitigate the risk, and it is from this assessment that decisions can be made about appropriate security and effective technology, including CCTV. Security Risk Assessments will benefit from specialist knowledge so assistance should be obtained from licensed, appropriately-qualified Security Professionals experienced in Security Risk Assessments.

Crime Assessment

CCTV (for security purposes) is usually selected to assist in managing some form of crime or unwanted behaviour. The type of crime or unwanted behaviour occurring will impact on: CCTV's potential to assist, where CCTV is located and how CCTV systems are designed. A Crime Assessment should be an early consideration during CCTV planning to assist in determining the types of crime occurring, how often they are occurring, where they are occurring and who the likely offenders are (eg. external threats, internal threats, professional criminals or opportunistic petty criminals, vandals, terrorists etc).

A Crime Assessment may include the collection and assessment of crime statistics, assessment of sites for local evidence of crime/unwanted behaviour, assessment of sites for environmental contributors to crime/unwanted behaviour, gathering anecdotal evidence from police and stakeholders, and assessing vulnerabilities to particular types of crime. This assists CCTV decision-making as it allows a determination of whether CCTV is likely to be effective against certain types of crime in particular applications. For example, CCTV may be more effective in locations where physical movement is limited because it is more difficult for potential offenders to avoid the cameras.

CCTV may be more effective against certain crime types due to their fundamental characteristics. For example, bank robbery can generally only be committed in the bank, so it is reasonably simple to locate cameras to provide footage of this crime type. However, crimes like graffiti that can occur anywhere may be more difficult to treat with CCTV. CCTV may be more effective against some types of offenders than others. For example, CCTV may deter a small-time, would-be-shoplifter who may be concerned about being caught, but it is likely to be less effective as a deterrent to an alcohol or drug-affected violent offender committing an assault. Crime Assessments can assist in an early determination of these types of issues to assist CCTV decision making.

Crime Assessments will benefit from specialist knowledge and experience so assistance should be obtained from licensed, appropriately-qualified Security Professionals.

Community Consultation

Formal consultation should be conducted and documented to assess perception of CCTV as a crime management tool. The community, staff members or other relevant stakeholders should be consulted early in the planning process to assess the potential privacy concerns, assess whether these groups are willing to support CCTV and to assess their knowledge of CCTV and perception of its ability to manage crime/unwanted behaviour.

If community consultation is not conducted prior to further CCTV planning/implementation, there is a risk that CCTV may be opposed by the community to a level that requires the system to be significantly altered or even decommissioned. Conversely, community expectations may be higher than the practical capacity of CCTV to achieve, leading to criticism and disillusionment.

Step 2 – Assess Suitability of CCTV to Manage Problems

Information to Support the Requirement for CCTV

CCTV can be an expensive strategy to implement so developing a strong case for its required use should be considered prior to expenditure. Information that may assist in supporting the requirement for CCTV may include:

- What type of crime/unwanted behaviour is currently occurring?
- How often does it occur?
- What is the average level of loss or consequence each time it occurs?
- Who is the offender?
- Will CCTV deter this type of offender?
- Whose responsibility is it for managing the risk?
- Will CCTV installation affect our reputation if ineffective?

This information may not be available if systems and process are not in place to gather and document such information. In order to maintain accurate, up-to-date information on which to base security expenditure, a comprehensive form of collecting and documenting crime/incident history records should be implemented and maintained.

Accurate records of this type will provide a basis for decision-making and will support a cost/benefit analysis for CCTV or other security strategies.

Cost/Benefit

During the planning stage of a CCTV system a cost/benefit analysis is recommended. Security (including CCTV) should be based on minimising loss or consequence after considerations of likelihood. Therefore, it is important to establish what the current loss level is, what the security measure will cost, and the level of savings the security measure is likely to afford. It makes sense to conduct a cost/benefit analysis prior to expenditure, to assess whether security measures (eg. CCTV) are able to minimise loss (or if the cost will actually exceed current loss). The cost/benefit analysis looks at what the total cost of the security measure will be per year (cost), and the likely benefits the system will provide (benefit). For example, a CCTV system may cost $100,000 to install, and then cost $10,000 per year (after first year) to manage and maintain. If the benefit derived from the system is estimated as being a 50% reduction in robberies due to prevention (currently incurring loss of $100,000 per year), an additional loss is made in the first year (due to the cost of implementing the CCTV), but over five years $140,000 will have been spent on CCTV, and $250,000 of loss (50% of robberies) will have been saved. The overall saving over five years is $110,000. In this example, the CCTV will have been a worthwhile investment.

As cost/benefit analysis provides only an estimate of future savings, it is also sensible to monitor performance to see whether projected costs and benefits are accurate and being achieved in reality.

It should be noted that loss can come in many forms. It could be in financial terms (dollars), or it could be harm (to people or reputation), or environmental damage. In some cases it can be difficult to quantify loss, such as fear of crime. Some forms of loss that are not financial may be able to be transferred into equivalent financial terms. For example, environmental damage may be translated into financial loss (eg. the cost of returning the environment to its pre-incident condition). Performing an "accurate-as-possible" cost/benefit analysis is better than not conducting one at all, as it will provide an indicative preview more likely to result in better decision-making.

A cost/benefit analysis to support CCTV may require information to establish estimated current levels of loss. This may include information such as: annual expenditure on remedial action (eg. graffiti clean-up), average financial loss per incident (eg. motor vehicle theft), how many such incidents occur each year, trends, perception of crime, likely consequences of adverse media attention etc. A cost/benefit analysis will benefit from specialist knowledge and experience so consideration should be given to obtaining assistance from licensed, appropriately-qualified Security Professionals.

Step 3 – Planning

Setting Objectives

The fundamental objectives of a CCTV system will determine where it is located, its design and ongoing management requirements. Therefore determining the fundamental objectives of a CCTV system should be an early consideration. For example, what problem is CCTV aimed at managing? If it is crime, what type of crime? Where and when does this crime occur? Who commits this crime? What image do we need to capture for CCTV to be of benefit? Is CCTV being used to deter crime, or is it being used to provide investigative information or is it intended to be used as evidence?

It is recommended that CCTV objectives be formally documented. It may be of assistance to develop a duty statement for each camera. For example, a single camera's duty may be to provide identification images of individuals as they walk through a particular door. Assistance with setting CCTV objectives should be sought from licensed, appropriately-qualified Security Professionals.

CCTV Policy and Procedure Considerations

A CCTV system may require formal written documentation outlining overarching policies and procedures to formalise responsibilities, compliance with legislation, how to maintain CCTV objectives, facilitate authorised use of the system and penalties for non-compliance.

The following sections outline some potential considerations:

Responsibilities

A CCTV Policy document should formalise who is responsible for each role involved with managing, operating and maintaining CCTV. This may include: who the owner of the system is, who is responsible for overall management of the system, who is responsible for operation of the system, who is responsible for integrity of information (recordings), who has access rights to view CCTV vision, responsibilities of monitoring staff, maintenance staff, the response force, etc. For further information see Section below: *Assessing Roles and Responsibilities.*

Non-compliance

A policy document should outline the penalties for non-compliant use of the CCTV system. This assists in deterring unauthorised use of the system and helps support compliance with legislation (if detailed in procedural documents).

Maintain Integrity of Data (Continuity of Evidence)

If CCTV footage is to be used for evidence, there are certain requirements for maintaining continuity of evidence to support the integrity of the evidence for use in court. Specific procedural requirements should be tailored to suit objectives in liaison with local police and once determined should be carefully documented in Standard Operating Procedures. Advice from State legal authorities should be sought to ensure that court requirements are also designed-in and met.

Signage

Policy documents should outline the extent to which signage will be used with the CCTV system. Specific signage requirements should be tailored to suit objectives and State legislative requirements. For more information on signage see section: *CCTV Signage Considerations*.

Securing Equipment

Policy and procedure documentation should outline the security requirements for CCTV infrastructure (eg. equipment, recording devices, storage facilities, control rooms etc), who is responsible for security, and how security will be maintained to ensure the integrity and privacy of information stored.

CCTV
For your personal safety and security CCTV cameras are in constant operation
Evidence can be used in a Court of Law

The fundamental objectives of a CCTV system will determine where it is located, its design and ongoing management requirements.

Compliance with Legislation

Policy and procedural documents should be tailored to outline how to use the system in accordance with relevant legislation. For example, if a particular organisation is required to store CCTV footage for a specific duration of time to comply with legislation, this could be detailed in Standard Operating Procedures to facilitate compliance.

Authorised Access

A CCTV policy document should outline who is authorised to operate CCTV, who is authorised to access stored recordings/recording infrastructure, who is authorised to make amendments to the CCTV Policy etc.

Training/Licensing

A CCTV policy document should outline any particular training required for operators or licensing requirements for installers, operators or consultants who may contribute to the system. Training may include how to use specific CCTV products (training by installer), or formal training (eg. Certificate in Security Operations). Licensing is required for installers of CCTV and Security Consultants who *"investigate or advise on matters relating to the watching, guarding or protection of property"* (*Security and Related Activities Control Act 1996*). Security guarding licenses may be required for monitoring staff. For specific licensing or training requirements contact WA Police Licensing Enforcement Division on 9223 7000.

Use of the Equipment

Policy and procedural documents should specify protocols on how CCTV equipment is to be used by operators. This should include how to use the equipment correctly, how to maintain security of equipment (eg. mobile cameras, recorded information), and what operators are (and are not) authorised to use CCTV for. This latter issue is important for facilitating compliance with privacy and other legislation.

Dealing with Complaints

Policy or procedure documents should outline how complaints about the CCTV system are to be dealt with. Staff or members of the community may wish to voice concerns about privacy or other system issues. Standard procedures should be developed to ensure complaints are dealt with as per the CCTV owner's policy.

Storage of Information

The storage of CCTV information (images) can have significant implications for owners and operators of CCTV. This depends on the size and complexity of the CCTV system. The policy document should outline the period of time for which CCTV images must be stored to comply with Commonwealth and State Archives legislation because the images are considered to be data or information in a legal sense. Australian Standard AS4806.1 recommends that a minimum of 31 days storage be achieved. Specific storage requirements may be regulated by a number of State and Commonwealth Acts. It is recommended that CCTV owners seek independent legal advice to ensure compliance.

Standards

Policy or procedure documents may outline the technical standards that a system is required to achieve. For example, minimum frame rates, resolution or methods of compression. For further information see Section: *Technical Considerations*.

The Western Australia Police has developed suggested minimum technical standards aimed at increasing the likelihood that CCTV footage will be of a quality that is more likely to assist police investigations. These suggested minimum standards outline suggested frame rates, resolution, storage and other technical information as a suggested guide.

Ongoing Review

Policy and procedure documents should be regularly reviewed so that performance can be measured and improvements and updates made as required.

WESTERN AUSTRALIA POLICE PREFERRED MINIMUM CCTV SYSTEM STANDARDS

	Preferred Minimum Standard
Visual	• When required, clear recognition of a standard vehicle number plate from the camera position. When required, clear recognition of facial features from the camera position appropriate to the installation.
Lighting	• Appropriate to achieve the visual standard at all times (day / night)
Movement activated lighting	• Ideally systems should incorporate a movement activated light inside the premises and/or outside the premises to assist in the capture of video and/or images of persons of interest under low light conditions.
Frame rate	• 10 Frames per second (FPS) (or higher) *Frame rate, or frame frequency, is the measurement of the frequency (rate) at which an imaging device produces unique consecutive images called frames. Frame rate is most often expressed in frames per second (FPS) and in progressive-scan monitors as hertz (Hz).*
Resolution	• 640 x 480 (or higher)
Camera/s	• Should support IP cameras as required. • *IP cameras are Closed-circuit television (CCTV) cameras that utilise Internet Protocol to transmit image data and control signals over a Fast Ethernet link. As such, IP cameras are also commonly referred to as network cameras. Progressive scan on camera Progressive or non interlaced scanning is a method for displaying, storing or transmitting moving images in which all the lines of each frame are drawn in sequence. Ideally, systems should have at least one camera located at eye level or close to eye level for capturing video and/or images of persons of interest. (Overhead cameras do not satisfy this requirement.)*
Embedded Information	• Time • Date, Camera identifier (number / name / position / etc)
Storage	• Stand alone storage system (not used for multiple purposes) Digital Held for a minimum of 28 days
Output	• At least one composite output *Composite video signal is typically connected using an RCA jack, normally yellow (often accompanied with red and white for right and left audio channels respectively). BNC connectors and higher quality co-axial cable are often used in more professional applications.*
File export	• One or more of the following: The system must be capable of burning to disk, in a simple operation: 1. The video file; and 2. the playback software required to view the video file In reference to (2.) above, "ideal" systems should export footage in a format which can be viewed on a standard Police computer, using readily installable software such as Windows Media Player, Windows Media Player Classic, or VLC Media Player, and should not require complex decoding software to play the footage. Systems which do not meet these requirements should comply with the requirements under "Software" below. The system should be capable of exporting enough footage to portable storage to enable location of the particular incident under investigation. Suitable portable storage should comprise of DVD, CD, external hard drive and/or flash memory in accordance with this requirement.
Software	• The playback software should: – Have variable speed control including frame by frame, forward and reverse viewing; – If the video file is from multiple cameras, the software should 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 recording from each camera to be searched by time and date. – Allow printing and/or saving (e.g. bitmap) of pictures with time and date. – The time and date associated with each picture should be legible. – Allow export to a removable media in a format that allows replay immediately.

Assessing Roles and Responsibilities

As part of the planning stage for a potential future CCTV system, it is important to undertake an assessment of the roles and responsibilities required to manage and run the system, and whether there are currently personnel available to undertake these roles/responsibilities or if new staff may be required. If insufficient personnel are available to support the ongoing management of a CCTV system, the system will be of limited benefit. The roles and responsibilities required will depend on the size of the system and its objectives, however, the following sections outline some potential roles/responsibilities to consider:

- A designated officer(s) responsible for the CCTV;
- Community liaison;
- Financing initial cost and ongoing cost of CCTV;
- Evaluation of system performance;
- Technical input;
- Tendering for installation, operation and maintenance;
- Selection of installer;
- Selection of operator;
- Selection of maintenance;
- Provision of training;
- Assessment of performance as a crime management strategy;
- Developing a system to deal with complaints;
- Development and ongoing review of a code of practice and standard operating procedures;
- Ensuring compliance with code of practice and standard operating procedures;
- Maintenance of CCTV, lighting, vegetation etc;
- Ensuring compliance with Australian Standards and Australian (and Western Australian) legislation;
- Development of CCTV specifications;
- Monitoring of CCTV (where required);
- Liaison with police and other authorities/owners;
- Procedure for the export of footage;
- Procedure to evidence that footage has not been tampered with (to ensure continuity/integrity);
- Response to incidents;
- Crime assessment (and evaluation of CCTV's effect on crime);
- Management of stored recordings.

Step 4 – Equipment and Installation

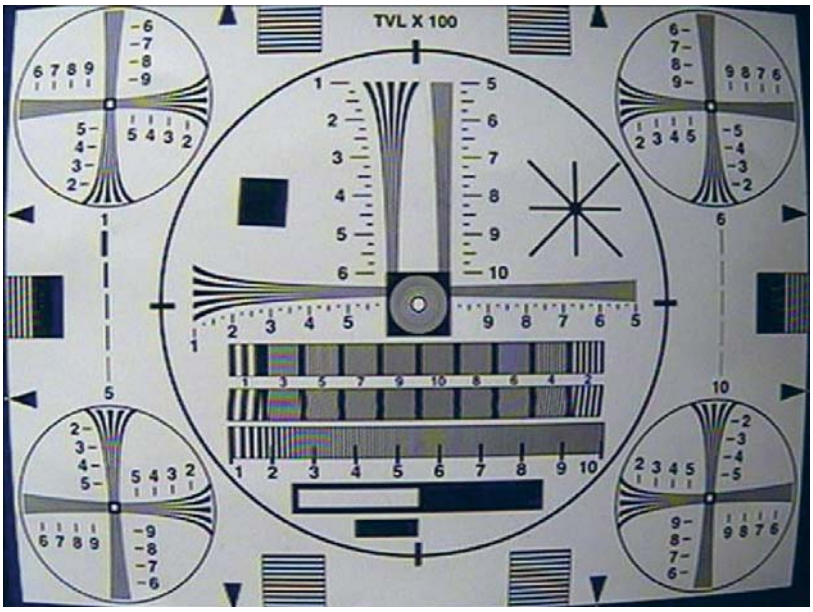
CCTV System Design

CCTV design benefits from technical knowledge as well as an understanding of local crime and security issues. Technical experience alone may produce a technically-proficient system which may not assist in managing location-specific crime. Conversely, experience with local crime and security issues and a lack of technical knowledge may produce a system that is aimed at achieving the right goals, but does not perform effectively from a technical point of view.

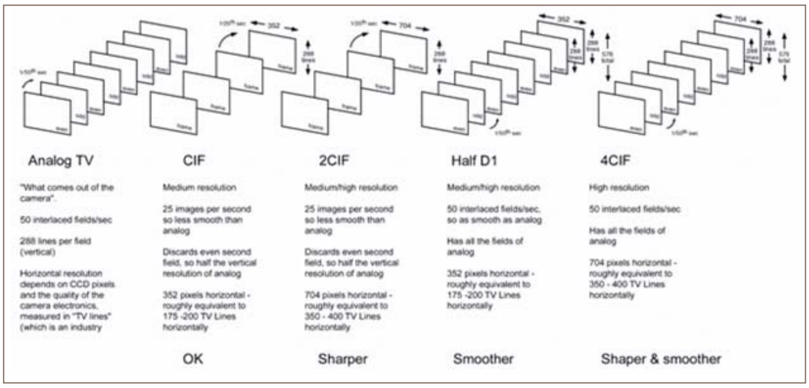
Only licensed persons can offer design services. Suppliers are not required to hold security licenses and therefore can only advise but not offer design services. It is recommended that prospective CCTV owners engage experienced Security Professionals to assist with design (if it does not already exist in-house). Installers should be able to demonstrate that they are suitably competent in system design.

Technical Considerations

There are many technical issues that must be considered as part of CCTV design. The following sections are not intended to provide a detailed understanding of the issues but rather as an introduction to the concepts requiring consideration. Further assistance with technical considerations can be sourced from licensed, qualified Security Professionals.



CCTV design must take into consideration the optimum balance between quality of images, number of images taken per second and storage space required to support objectives.

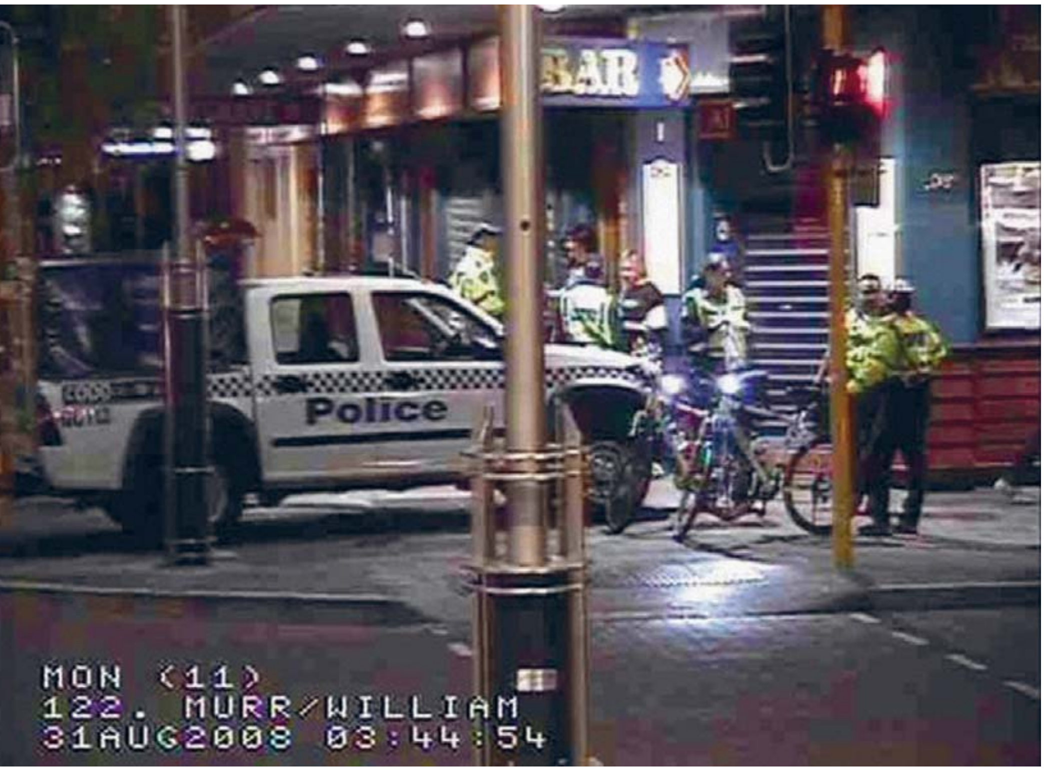

Analog TV
"What comes out of the camera".
50 interlaced fields/sec
288 lines per field (vertical)
Horizontal resolution depends on CCD pixels and the quality of the camera electronics, measured in "TV lines" (which is an industry
CIF
Medium resolution
25 images per second so less smooth than analog
Discards even second field, so half the vertical resolution of analog
352 pixels horizontal - roughly equivalent to 175 -200 TV Lines horizontally
OK
2CIF
Medium/high resolution
25 images per second so less smooth than analog
Discards even second field, so half the vertical resolution of analog
704 pixels horizontal - roughly equivalent to 350 - 400 TV Lines horizontally
Sharper
Half D1
Medium/high resolution
50 interlaced fields/sec, so as smooth as analog
Has all the fields of analog
352 pixels horizontal - roughly equivalent to 175 -200 TV Lines horizontally
Smoother
4CIF
High resolution
50 interlaced fields/sec
Has all the fields of analog
704 pixels horizontal - roughly equivalent to 350 - 400 TV Lines horizontally
Shaper & smoother
352
704
288 lines
576 total

Resolution

Resolution refers to the quality of the pictures that CCTV cameras produce. This is similar to the varying resolutions available using still-picture digital cameras. The higher the resolution a camera can take the better the original picture quality is. Resolution for CCTV is often discussed in terms of CIF (Common Intermediate Format). CIF is a standard image format that equates to 288 lines of information with 352 pixels per line. QCIF (or quarter CIF) is equal to 176 x 144, 2CIF is equal to 704 x 288, and 4CIF is equal to 704 x 576. The original resolution is reduced once the original images are compressed for storage (sometimes significantly reduced depending on the compression format used). Compression is used to compact information so that a longer duration of footage can be stored. The more images are compressed, the more can be stored, however image quality is sacrificed. CCTV design needs to take into consideration the optimum balance between quality of images, number of images taken per second (frame rate) and storage space required to support objectives.

Frame Rates

Frame rates refer to how many pictures a camera system is ‘taking’ per second (frames per second or fps). Most camera systems have variable frame rates so they can be set to take anywhere from 25 frames (pictures) per second to 1 frame every few seconds. Some applications of CCTV may require higher frame rates to ensure that vital images are recorded for investigative or evidential purposes. For example, cash counting may require high frame rates to ensure that fast movements are caught on camera. The higher the frame rate, the more information is usually being recorded. Therefore, higher frame rates generally mean that more storage space is required. CCTV design needs to take into consideration the optimum balance between quality of images, number of images taken per second (frame rate) and storage space required to support objectives. For example, frame rate may not be as



important as resolution in a given situation if the objective for a camera is identification.

Compression

Compression refers to the reduction of redundant information within images to reduce the amount of data for transmission and/or storage of images. There are many compression types that can be used, each of which will compress images using different techniques and by differing amounts. Most compression techniques seek to remove unnecessary data/detail without reducing how an image generally looks, however, too much compression can significantly effect how the original image looks, even to the extent that it may be unusable for investigative/evidential purposes. For example, excessive compression may hamper the ability to adequately identify faces. Compression methods selected should be a carefully considered balance between optimum image quality and file size for storage. For more information see Section: WA Police Preferred Minimum Standards.

Day/Night, Inside/Outside

CCTV needs adequate lighting levels to provide quality images. A key consideration therefore is whether the objectives of the CCTV require it to survey space/individuals during the day or at night (or both), inside or outside (or both). If CCTV is required to survey outdoor areas at night and provide colour images to meet objectives, adequate external lighting must be factored into the design.
If objectives require accurate colour rendition to support investigative/evidentiary purposes, CCTV should be supported with appropriate white lighting that produces images that depict accurate colours. Some cameras are able to capture images in near darkness; however these generally operate only in black and white at that time. Some cameras operate by viewing the infrared spectrum and can detect individuals in the dark; however the images of people may appear ghost-like and may support varying degrees of recognition or identification of the individual. CCTV design must therefore take into account system objectives, the environment cameras will operate in and the lighting conditions required for successful operation.

CCTV design must take into account system objectives, the environment cameras will operate in and the lighting conditions required for successful operation

Lamp type	Lumens per watt	Average life hours	CRI	Colour rendition	Operating cost	Colour temp range (deg, K)
Incandescent	15–20	750–1K	100	Excellent	High	2750–3400
Halogen	18–25	1K–3.5K	100	Excellent	Above average	2850–3000
Fluorescent	55–100	7.5K–24K	51–95	Good–excellent	Average	2700–7500
Mercury vapor	40–60	16K–24K	20–60	Poor–good	Average	3000–7000
Metal halide	80–125	5K–20K	60–80	Very good	Below average	3200–3700
H.P. sodium	75–140	10K–24K	20–80	Good–excellent	Low	1900–2700
L.P. sodium	Up to 200	14K–18K	0	Poor	Low	1700

Tests

Sometimes the technical requirements of CCTV to support objectives may be difficult to predict accurately due to site-specific conditions or special applications. Testing can be a way to assess whether assumptions regarding technical requirements of CCTV will meet objectives. For example, if a CCTV system needs to be able to clearly display a vehicle license plate number at a 25 meter distance, a test camera could be set up under local conditions with a mock-up license plate used to assess the required resolution. Similarly, testing may assist in determining potential issues, for example, light conditions such as the position of the Sun could affect CCTV vision significantly. Testing should be carried out under the same conditions in which the CCTV system is required to support objectives (eg. time/location/lighting/environment).

WA Police Preferred Minimum Standards

Police note that the quality of recorded CCTV images is a vital element if CCTV is to provide information to support investigation or evidence of crime/unwanted behaviour. In an effort to facilitate quality of recorded footage, WA Police have developed as a suggested guide, the *WA Police Preferred Minimum Standards* for CCTV images. These suggested minimum standards provide guidance for CCTV owners on technical settings for producing images that are more likely to be of value to police. General enquiries to police can be made by phoning 131 444.

Storage (DVRs, Retention Time)

Storage refers to the method and duration of keeping recorded CCTV images. CCTV used to be recorded on VHS (or S-VHS) video tape recorders and stored on video tapes. These days, CCTV is generally stored digitally using hard drives, DVRs (Digital Video Recorders) or NVRs (Network Video Recorders). If footage needs to be stored more permanently it is usually transferred to DVD (disk). Storage time refers to the amount of time that CCTV images can be stored on a given medium before it is recorded over. For example, a DVR may be able to store CCTV footage from 4 cameras for 14 days before the storage space is full and recordings start to be recorded over. CCTV design must take into account objectives of the system, required storage times to support objectives and storage times determined under Commonwealth and State archives legislation. Consideration should be given to the installation and use of redundant DVRs.

Fixed cameras that are installed outdoors need to withstand the weather, wind loading and environmental conditions.

Fixed and Mobile CCTV

CCTV cameras can either be fixed (eg. non-moveable from location to location, although they can pan/tilt and zoom) or mobile (eg. re-deployable, either mounted in a vehicle or building for a period of time and then relocated as required).

There are issues that should be considered for both fixed and mobile CCTV. The following sections discuss some of these issues:

Fixed Cameras

One of the main considerations for fixed cameras is displacement. Displacement means that crime may change location (away from CCTV), change the time it occurs or the crime type may change. Since fixed cameras are not easily moved it makes it simpler for offenders to avoid areas with CCTV. For more information about displacement see Section: *Strengths and Limitations of CCTV*.

Another consideration is that fixed camera infrastructure such as camera poles, lighting, power, transmission links, recording facilities and monitoring facilities are more permanent in nature and therefore can be quite expensive.

Fixed cameras that are installed outdoors need to withstand the weather, wind loading and environmental conditions. Depending on where they are located they may require special housings, anti-climb devices, purpose built poles, or other ancillary devices.

Where poles are used for the dual purpose of CCTV and lighting, or where a power supply runs along a pole which is also used for situating a CCTV camera, the CCTV camera may be affected by the power source's electro-magnetic field. This may affect the quality of the system. A qualified and licensed CCTV installer should take this into consideration during the design and installation of the system.

Mobile Cameras

One of the main considerations for mobile CCTV systems is the security of mobile cameras. Mobile cameras are often small portable units, sometimes configured in a briefcase arrangement. Their size and portability means that they are more vulnerable to theft or tampering. Mobile cameras should be located in secure areas or be accompanied by monitoring personnel to minimise the risk of theft or damage.

Another consideration regarding mobile CCTV is how to use signage with the cameras. Signage is one method to communicate its use in an area and contribute to CCTV's deterrent value by creating awareness. Signage used with mobile camera systems is likely to also be re-deployable and therefore may also be vulnerable to theft or tampering.

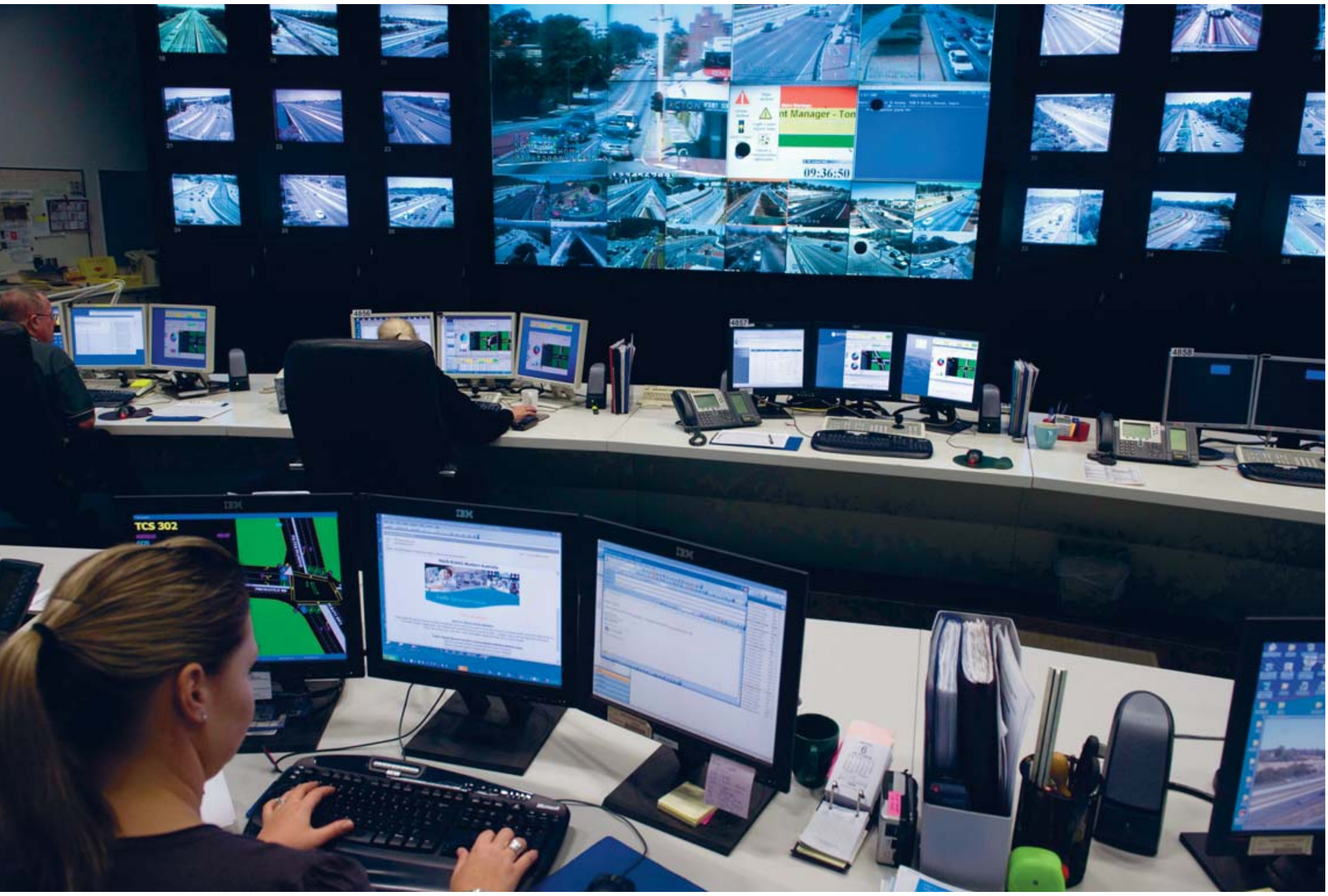
Consideration needs to be given to where signage will be located and how it will be fixed so that it is highly visible but also secure (for more information on signage see Section: *CCTV Signage Considerations*).

Another consideration for mobile cameras is whether they will be recorded (only) or monitored (for more information see Section: *Monitored CCTV and Recorded CCTV Considerations*). Mobile cameras that are required to be remotely monitored may require a secure Internet landline or wireless connection.

Mobile cameras should be located in secure areas or be accompanied by monitoring personnel to minimise the risk of theft or damage.

Trial Sites

Depending on the level of information available to achieve effective CCTV planning, trial CCTV sites may be considered to test the effectiveness of CCTV prior to significant further investment. For example, if a prospective CCTV owner has no experience with CCTV, has no existing CCTV or does not have sufficient information on which to base the likely performance or success of proposed CCTV, trial sites may provide important data that may contribute to further CCTV decision-making. A trial site may involve setting up a temporary camera system to assess its performance against objectives, performance in a particular area or performance in managing a particular type of incident.



Monitored CCTV is more likely to contribute to detection of incidents/offenders and initiate responses to incidents in progress

Monitored CCTV and Recorded CCTV Considerations

One major design decision for a CCTV system is whether cameras will be monitored (and recorded), or recorded only. The decision to monitor or record CCTV should be based on system objectives as this decision will impact significantly on system performance and costs.

Monitored CCTV means that cameras are actively watched by personnel in real time. Monitored CCTV is usually also recorded. CCTV may not be actively watched by personnel, but instead images are recorded so that any incidents that occur within the field of view can be later reviewed.

The benefits of monitored CCTV are that it is more likely to contribute to detection of incidents/offenders and initiate responses to incidents in progress. This also contributes to its deterrent value. Appropriate monitoring and response planning is important to realise these benefits. Actively monitored CCTV systems may also consider use of a PA system to allow monitoring staff to directly communicate with, or warn, would-be offenders.

This is area regularly monitored by Safety Cameras making a safer city

CCTV owners should use signage to indicate to the public that their activities within an area may be observed and recorded.

Conversely, the disadvantages of monitored CCTV are the potential additional infrastructure and personnel required to support it, the potential ongoing costs of maintaining transmission links and employ monitoring staff, and the natural inclination of humans to become oblivious to routine screen information. These issues may be especially significant in larger systems (eg. public area video surveillance) that may require more resources (and cost) to implement and maintain.

The benefit of recorded CCTV is that it provides images that may assist in post-event investigation or potentially as evidence in court. The limitation of recorded-only CCTV is that it is unlikely to initiate a response to an incident, and therefore may have limited deterrent value to offenders.

CCTV Signage Considerations

Why use Signage with CCTV?

Although the use of covert CCTV is not illegal in Western Australia, CCTV owners are required to abide by the legislative requirements outlined within the *Security Devices Act 1998*. Although there is no obligation requiring the use of signage under the current Act, CCTV owners should use signage to indicate to the public that their activities within an area may be observed and recorded. This is particularly important for internal environments (inside buildings and businesses). It is recommended that owners of CCTV systems seek legal advice to ensure compliance with Australian and Western Australian Legislation to avoid potential privacy and other legal issues.

Australian Standard *AS4806.1 – 2006 Closed Circuit Television – Management and Operation* states that (as a minimum) CCTV signage be posted at all CCTV system site entries.

CCTV signage also plays a part in deterring would-be-offenders by highlighting that CCTV is in use.

Signage at face level may be more easily noticed, but signage mounted higher may assist in preventing vandalism ...

Ownership

CCTV signage should clearly communicate ownership of the CCTV. Contact details should also be considered to facilitate feedback, complaints or reporting problems/damage. Owner's symbols may also assist in providing Territorial Reinforcement (in other words, indicators of ownership, an element of Crime Prevention Through Environmental Design – CPTED or Designing Out Crime).

Wording

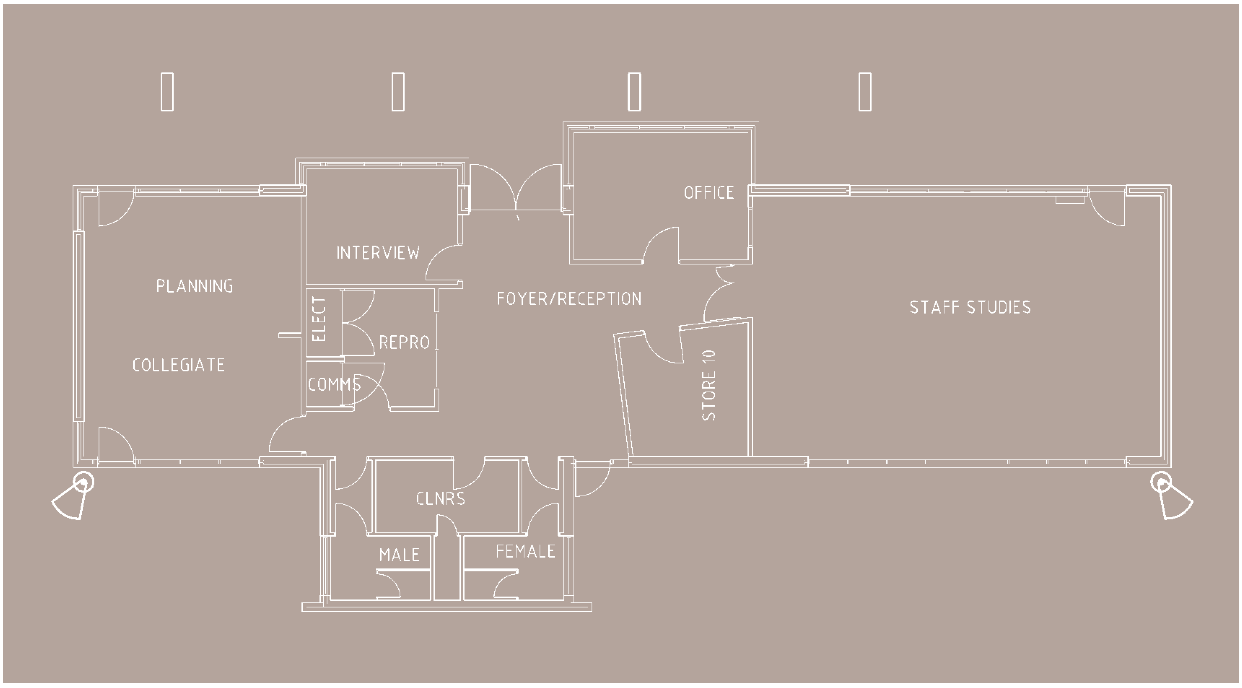
It is recommended that the wording used on CCTV signage be carefully selected and accurate. For example, if CCTV is not monitored (being actively watched by a person in real time) signage should not infer that the CCTV is being monitored.

Overstating the capability of CCTV to increase its crime-deterrent-value is tempting; however, it can also lead to the creation of a false sense of security resulting in members of the public potentially putting themselves at risk. It could also negatively affect the community's perception of the usefulness of the system, particularly if signage states or implies that the system is highly sophisticated and effective, when in fact, its technical performance may be poor.

Sign Placement

Australian Standard *AS4806.1 – 2006 Closed Circuit Television – Management and Operation* states that (as a minimum) CCTV signage be posted at all CCTV system site entries. Determinations on the use and location of signage should be made on a case by case basis giving adequate consideration to issues of safety and practicality.

Signage at face level may be more easily noticed, but signage mounted higher may assist in preventing vandalism, theft or graffiti. Signs should also be placed in areas with sufficient lighting to ensure that signage is visible and legible at all times and consideration should be given to treating signage with anti-graffiti coatings to facilitate graffiti-removal, and UV stabilization to prevent fading in sunlight.



Other Considerations

Consideration should be given to methods of ensuring that CCTV signage will be understood by everyone, particularly individuals who may not be able to read, have poor eyesight or do not understand English. For this reason consideration should be given to including both symbols and bold lettering on signage.

Awareness campaigns can assist in alerting the public (and offenders) to the introduction of CCTV systems, and to be alert for CCTV signage.

Locating and Securing Cameras

Cameras need to be located in an optimum position to provide the images required to achieve the system's objectives. An example of a building plan indicating the location of CCTV cameras (at each end of the building) is displayed above. It is recommended that building plans showing the locations of all CCTV cameras and their intended fields of view are produced and included as part of the owner's CCTV policy documents.

As far as practical cameras need to be protected against loss or disruption to service. Potential risks to cameras may include theft, vandalism or local conditions affecting their performance. Consideration should be given to locating and securing cameras to minimise loss or disruption. The following sections discuss some considerations:

Mounting Height

Mounting heights for each camera must support the camera's objective so that it can provide the scene required. Cameras should be mounted no higher than 8-9m above the ground. Where possible, cameras should be mounted at a height that also supports security so they are more difficult to access by thieves or vandals. Another consideration for mounting-height is maintenance. Cameras should not be mounted in areas that make them too difficult to access for regular maintenance.

Overlapping Cameras

Ideally, the field of view of each camera in the system should overlap so that no blind spots are created in the areas requiring camera coverage. Camera security is supported by a system design which locates cameras in a way that allows each camera to be "seen" by another camera. This form of design makes it more difficult for offenders to access or vandalise cameras "unseen".

Locating Cameras in Secure Areas

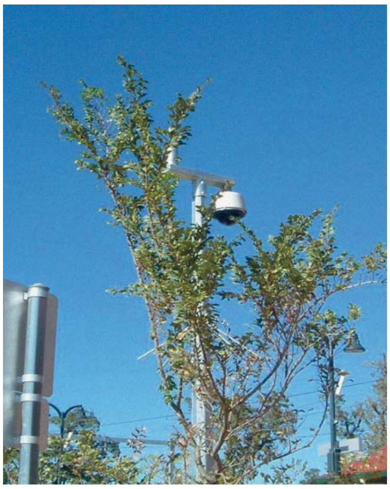
If possible cameras should be located in areas that cannot easily be accessed by offenders, thieves or other potential threat sources, such as within secure perimeter fencing.

Alarm Systems

Additional protection can be provided to a CCTV system by tempering cameras into the site's security alarm system. Should a camera be vandalised, attacked or tampered with, the site's alarm system will activate. Alarm responses can be programmed by the system owner to create an audible alarm, alert a security company or cause other cameras in the system to focus on the camera being attacked.

Camera Housings

Camera housings come in two general categories: shoebox housings or dome housings. Housings assist in protecting cameras from the weather, dust and potential vandalism. Domes can assist in obscuring the direction the camera is pointing which may have an additional deterrent effect.



Anti-climb Devices

Anti-climb devices such as spikes can be fitted to camera poles to deter climbing and therefore access to cameras by vandals or thieves.

Maintenance

Location and mounting of cameras should take into consideration ease of access by maintenance personnel. If cameras are located in areas or mounted in ways that make it too difficult for authorised access by maintenance personnel it may hamper regular maintenance, cleaning or corrective action to cameras that have slipped out of alignment.

Wind

Cameras programmed with VMD (Video Motion Detection) should be secured in such a way that wind pressure does not cause movement that the camera interprets as movement in the field of view. Consideration should be given to supporting rods in these circumstances to avoid nuisance alarms.

Avoid Glare

Location and mounting of cameras should take potential sources of glare into consideration. In the same way that glare can affect an individual's ability to see (for example, looking into the Sun), glare can affect the ability of cameras to produce clear pictures of a scene. When locating cameras care should be taken to avoid directing cameras toward bright light, reflective surfaces or the Sun.

A holistic system requires supporting strategies to further support deter and detect roles, and to provide the functions of delay and respond.

Supporting Infrastructure/Measures

CCTV may be of limited value if used alone. Other security or crime prevention strategies are usually required to support a holistic system, ideally to accomplish all the roles of Deter, Detect, Delay Communicate and Respond (for further information see Section: *Strengths and Limitations of CCTV*). CCTV may partially fulfil the role of deterring crime or unwanted behaviour, and potentially detecting crime if it is monitored. A holistic system, however, requires other supporting strategies to further support deter and detect roles, and to provide the functions of delay and respond.

Other supporting strategies that should be considered for supporting CCTV may include:

CPTED or DOC

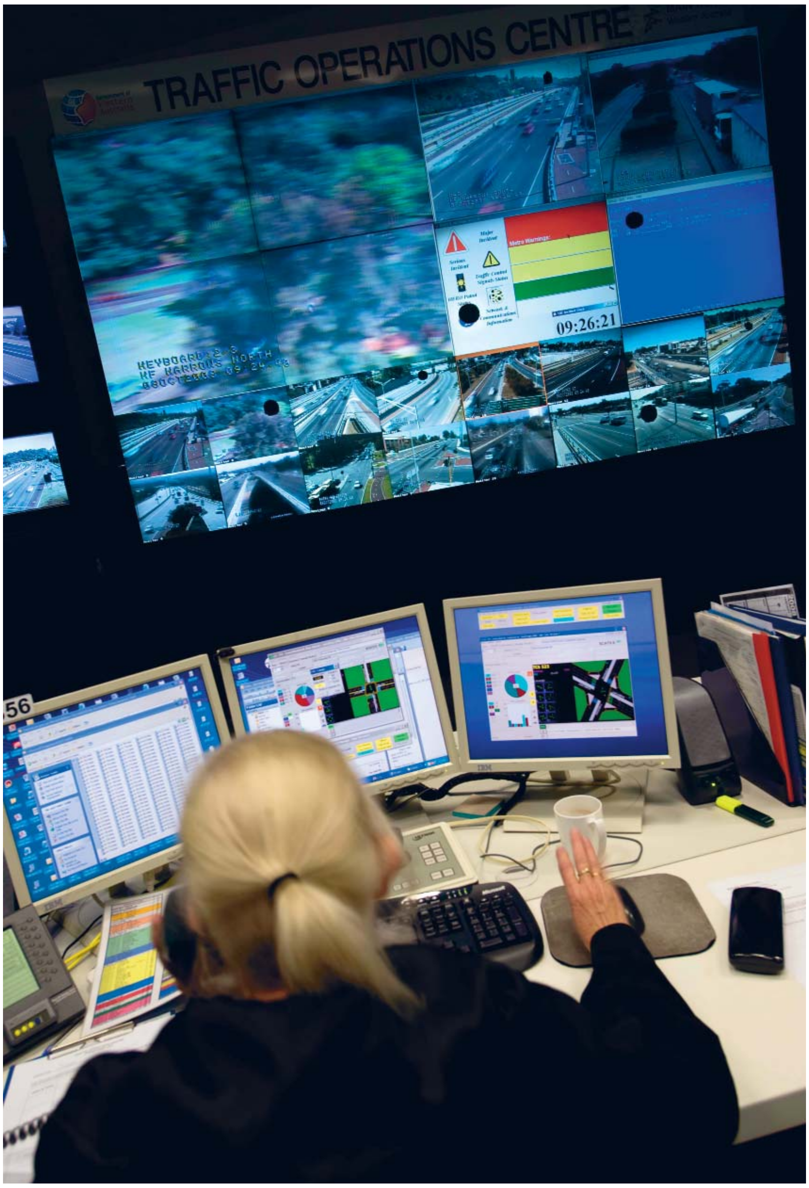
Crime Prevention Through Environmental Design (CPTED) also known as Designing Out Crime (DOC) is a crime prevention approach that may offer an alternative or supporting strategy for CCTV. CPTED uses the built environment to influence behaviour, deter crime and encourage use of space by authorised users of a space. The main principles of CPTED are Natural Surveillance, Natural Access Control and Territorial Reinforcement. More information about CPTED or DOC strategies can be sourced from the Office of Crime Prevention website (http://www.crimeprevention.wa.gov.au/). CPTED strategies will benefit from specialist knowledge and experience so consideration should be given to obtaining assistance from licensed, appropriately-qualified CPTED Practitioners.

Lighting

Studies on lighting have shown that it can deter some types of crime in certain circumstances and encourage use of space by the community due to creating an increased perception of safety. Lighting may have its own crime prevention qualities, but it is also a vital element in a CCTV system by assisting cameras to produce clearer images. If colour accuracy in CCTV recorded images is necessary to ensure that the objectives of the CCTV system are met, consideration should be given to supporting cameras with lighting that will provide a white light with good colour rendition.

Monitoring

Monitoring has a specific meaning within CCTV terms. It refers to the active, live watching of CCTV vision by people whose role it is to supervise the places being watched. Some CCTV systems are not monitored, but are recorded only. Monitoring of CCTV generally requires additional equipment, infrastructure and personnel to achieve, all which incur an additional cost. Monitored CCTV systems are more likely to deter crime/unwanted behaviour, but only if monitoring is able to effectively detect incidents and prevent the incident from occurring or initiate an effective response.



Actively monitored CCTV systems may include a PA system to allow monitoring staff to directly communicate with (or warn) would-be offenders, to enhance the systems crime deterrent value. Actively monitored systems must also have consideration for a suitable response force to manage incidents. Whilst these strategies do enhance the crime prevention capability of a system they also require additional cost and resources to achieve.

If an offender hid their identity (eg. with a balaclava) to avoid being identified, a monitored CCTV system may still be able direct a response that results in the offender being apprehended. Conversely, a recorded-only CCTV system may not pose a problem to an offender in this scenario, as an immediate response is unlikely and recorded footage may not be sufficient to identify the offender.

It should also be noted that if cameras are not monitored there is a risk that they could be inoperable for considerable time before a potential problem is recognised. Regular inspections/tests should be considered to assist in managing this potential issue. Consideration should be given to CCTV tools that generate an alert for operators if a camera becomes inoperable.

Intruder Detection

Intruder detection includes technologies such as alarm systems, intrusion sensors, fence detection systems and electric security fences. These technologies are designed to initiate an alarm if an intrusion is detected. Intruder detection can assist the role of detection. It can also be used to support CCTV. For example, CCTV recording could be activated by an alarm input from an intruder detection system, or it could alert a response capability.

Video Analytics

Video analytics is the use of logical processing (usually IT based) to assist in the analysis of video information for specific data, behaviours or objects through activities such as the programming of cameras to automatically 'patrol' fildes of view, detecting movement in a surveyed CCTV scene, recognising objects in a scene, recognising some unwanted behaviours (eg. moving into a particular area), and initiating an alarm when certain conditions are met (eg. to start recording footage, or to alert staff of an issue).

Video analytics may be of use to

assist monitoring staff to recognise a range of issues or to save on CCTV storage space. Video analytics developers continue to design new functions; however, it is recommended that trials be conducted to establish whether video analytics will perform adequately for a given application in a particular location. It should be noted that video analytics is not recommended as a substitute for human monitoring.

Access Control

Access control refers to systems that limit the movements of individuals. Examples include: natural barriers, doors, swipe card systems and keying systems. It is easier to predict where cameras need to be located in order to capture the required images (eg. an identification image of an offender) if CCTV is supported by access control.

Physical Security

Physical security such as fences, barriers, locks, doors and gates may support CCTV by providing a delaying role. Physical security should be designed to delay an offender once they have been detected, so that a response can be effectively achieved before the offender can achieve their target and escape. Physical security may be of assistance to slow an offender down in order to capture clear CCTV footage of them.

Communication and Response

If no response capability exists to react to an incident or crime, then offenders may not be deterred from offending or apprehended during an incident. A response is the final important link in an effective integrated security system. Response to an incident may be enacted by security staff or police.

Operation

Control Room Considerations

Monitored CCTV systems with significant numbers of cameras may require a dedicated CCTV monitoring or control room. The following sections discuss some considerations:

Space

A dedicated monitoring facility requires a suitably sized room or floor-space. This could represent a significant cost if it does not already exist or if it requires significant alterations/refurbishment to achieve. A monitoring facility needs to provide adequate room for infrastructure to support the CCTV system and monitoring staff potentially including racks for recording equipment, rows of monitors and control equipment, furniture, toilets etc, and room for potential future expansion.

Security/Construction

A CCTV monitoring facility may house staff, sensitive information and significant assets including valuable or sensitive equipment and the facility itself may represent a key element in ensuring organisational security or business continuity. For these reasons, consideration should be given to the physical construction of the facility and its ability to support the security of staff, information and assets and non-disruption to operations. Considerations may include: physical construction (robust buildings materials), CPTED, defence in depth, barriers, solid core doors and robust door furniture, electronic access control, and intruder detection. Security construction may be determined through a formal Security Risk Assessment process. Assistance with Security Risk Assessments should be obtained from licensed, qualified Security Professionals.

Ergonomics

Ergonomics and staff comfort is important as monitoring staff may spend extended hours in front of monitors, and if uncomfortable, may not be able to concentrate on operations. Staff should be seated comfortably, able to reach control equipment comfortably, and view monitors from an optimum distance without having to continually refocus their view to compensate for monitors located at varying distances away. Ideally monitors should be laid out in an arc so that all monitors being viewed from one point are the same distance away from the viewer.

Staff

Depending on the number of hours CCTV is monitored, staffing may require numerous shifts. A 24 hour monitored facility may require three overlapping shifts for around-the-clock monitoring. A consideration here is the ability of staff to perform adequately over extended periods of time. Some research suggests that an individual's attention span significantly reduces after 1 hour of continuous viewing of monitors. Monitoring staff may need to work in pairs to allow 1 hour active monitoring sessions taken in turns. Working in pairs also facilitates having at lease one staff member available for monitoring at all times (eg. during toilet breaks etc).

Training may be required for monitoring staff depending on organisational policy and local legislation. Monitoring staff may require a Security Officer's License if they are someone: *"who for remuneration watches, guards or protects any property"*

Reference: Security and Related Activities (Control) Act 1996 (WA).

Elective training is available to assist monitoring staff such as elective units as part of a Certificate III in Security Operations. Enquiries regarding specific training or licensing requirements for a particular application can be directed to Police Licensing Services.

Liaison with Police

CCTV system owners will generally liaise with police at some point following an incident caught on camera. For larger CCTV system owners, liaison with police may occur at the outset of considering or developing a CCTV system, so that police can contribute in a two-way partnership. Police may also be able to partner with owners of larger CCTV systems to conduct specific investigations or operations using CCTV. Police may be able to offer or guide owners toward sources of information or professional advice (through licensed Security Professionals) that will assist the effectiveness of a CCTV system. Information may include crime statistics or specific crime hotspots, or information regarding storage mediums (for CCTV footage) to facilitate ease of transferring recorded images to police.

Liaison with police will also assist in developing a standard method for contacting police and arranging for retrieval of recorded images to maintain continuity of evidence. Should police require CCTV footage from a CCTV owner as part of an investigation they may request that the owner provides it voluntarily or may compel the owner to provide it via a warrant.

General enquiries to Police can be made by phoning 131 444 or the Office of Crime Prevention on 9222 9733.

Further assistance should be sought from licensed, qualified Security Professionals.

The WA Police have recently launched *Blue Iris*, a register of WA based CCTV systems aimed at mapping the locations of CCTV systems than can be used by police investigators. **Owners of CCTV systems can register their system with Blue Iris on line (https://blueiris.police.wa.gov.au/).**

Information Security Considerations

The use of CCTV generally results in the storage of large quantities of stored information (CCTV images). This information may be stored on hard drives, on DVD (disks), or in hardcopy (paper documents). CCTV images may be extremely important due to their sensitivity. If sensitive images were leaked by any means (for example onto a website or to the media) it could have severe consequences for the CCTV owner. For this reason Information Security strategies should be considered to classify information (eg. what is and is not important, and what level of protection each category needs), clearance for individuals (eg. determine who needs access to information based on "need to know"), and a means of controlling access to information. This may be supported by: logical access control, physical access control, physical security, information handling policies and procedures.

Other sources of information relating to a CCTV system may also warrant Information Security strategies. Documented policy and procedure documents or CCTV design documents may include detail about a CCTV system that may be of benefit to offenders because it could indicate system weaknesses. Similarly, access to CCTV monitoring points may provide detail about where CCTV cameras are located and what they are able to view.

Incident Management

CCTV can be an effective incident management tool if it forms part of an integrated system that performs the roles of deter, detect, delay communicate and respond (for further information see Section: CCTV's Role in Security). Incident management may employ monitored CCTV with audio capability as a means of deterring offenders. For example, if potential offenders are seen (via CCTV) to be engaging in unwanted behaviours, they can be warned via an audio system remotely by monitoring staff from the CCTV monitoring point. Potential offenders could be tracked by monitoring personnel using Pan-Tilt-Zoom cameras and if a response is required, monitoring personnel could alert and guide responding security personnel to the persons of interest. Recorded images of offenders could then be used to support apprehension and potential conviction of offenders.

Maintenance

CCTV requires ongoing maintenance and regular inspections to ensure the system is performing effectively. Maintenance may include cleaning, repairing or replacing camera components, but it also may include maintenance of lighting or surrounding vegetation that may impact on CCTV performance. Maintenance should only be undertaken by qualified and licensed personnel. CCTV planning should take ongoing maintenance budgeting into consideration.

Maintaining Vegetation

Vegetation in the vicinity of cameras can affect the performance of CCTV. For example, trees or other forms of vegetation may obscure CCTV vision, or if VMD (Video Motion Detection) is used with the CCTV, vegetation that moves in the breeze may trigger VMD alarms or initiate recording of footage when it isn't required. For these reasons, ongoing management of vegetation may be required to support CCTV. Maintenance of vegetation may also prevent trees obscuring lighting which could affect CCTV performance.

Repairing and Replacing Cameras

CCTV cameras may need to be repaired or replaced, potentially due to a number of reasons including:

- Theft of cameras,
- Vandalism,
- Broken, dysfunctional or superseded cameras.

Ongoing costs for replacement of cameras is dependent on a number of issues, including:

- The type of cameras selected (and therefore being replaced),
- The extent of damage (eg. camera only, camera and expensive lens, camera and camera pole),
- Labour required to replace the camera,
- How often cameras require replacing (potentially due to number of incidents per year that affect the cameras, eg. theft).

Some of the above criteria may be unknown prior to CCTV installation. For example, how often cameras are likely to be the target of theft/vandalism.

A Crime Assessment may assist in determining likelihood of damage to cameras or to assist in locating/securing cameras to minimise damage (See Sections: *Risk Assessment and Crime Assessment*).

Consideration should be given to permanently identifying cameras with the owner's name and telephone number to reduce the resale potential in the event of theft. Owners should also consider documenting camera serial numbers.

Cleaning Cameras

Cameras may require regular cleaning due to dust, graffiti, insect infestation, being located near the coast, sea/air, etc. Scheduling for cleaning should be determined on a case-by-case basis, depending on the local environmental conditions.

As a minimum, cameras should be cleaned and maintained 6 monthly, including but not limited to:

- Cleaning dust,
- Checking seals,
- Checking cooling fans,
- Lubricating servo motors.

Other maintenance may include:

- Changing belt drives approximately every 2 years (if applicable),
- Changing cooling fans approximately every 2 years (if applicable),
- Assessing whether domes need replacing every 3 to 5 years (if applicable).

Legislation

Privacy Considerations

CCTV can be used to record images of people and places. Several laws exist locally and nationally that may impact the extent to which such potentially private information can be legally recorded. Breach of some legislation incurs significant penalties, so consideration of all potentially applicable laws is a vital consideration at the outset of considering the use of CCTV.

A determination of the extent to which CCTV can be legally used may affect decision-making regarding: whether CCTV will be used at all, the design of a CCTV system, location of cameras, use of CCTV signage, and development of CCTV policies and procedures.

As Western Australia does not have a Privacy Act, the use of surveillance devices is regulated by the *Surveillance Devices Act 1998 (WA)*. This legislation prohibits the recording of "private activity".

Private activity means "any activity carried on in circumstances that may reasonably be taken to indicate that any of the parties to the activity desire it to be observed only by themselves." (S3 SDA)

Activities carried on in circumstances where it should reasonably be expected that the parties may be observed or overheard are not considered private.

It is essential to consider the surrounding circumstances, including the location and physical environment, in determining whether the use of CCTV will breach the *Surveillance Devices Act 1998*. When planning to install CCTV, owners and/or operators should ask themselves:

(a) Is it likely that the CCTV will record activities that people might reasonably desire to be observed only by themselves?

(b) Is the CCTV system observing an area where people ought to reasonably expect that their activities might be observed?

Provided that CCTV cameras are positioned to observe public locations in which it might reasonably be expected that activities taking place in those areas be observed, and provided that CCTV cameras are not placed in locations or used in such a way as to suggest that the intention of camera's placement or use is to observe private activity, there would be no breach of the Surveillance Devices Act 1998.

It is therefore advisable that CCTV system owners develop a duty statement and document the principle purpose of each camera within their CCTV system. It is also advisable that CCTV owners utilise signage to make people aware that their activities within an area may be observed and recorded.

Owners of CCTV systems should inform themselves of the laws that may impact on their use of CCTV prior to planning a system, and that ongoing identification and review of local and national laws be regularly conducted.

Source: Advice to Western Australia Police Communications by State Solicitor's Office.
April 2009.

Step 5 – Implementation

The technical installation of the CCTV system should only be undertaken by a licensed and trained system installer. The Security Agents Institute of Western Australia (SAIWA – www.saiwa.asn.au) and the Australian Security Industry Association Limited (ASIAL – www.asial.com.au) can provide lists of licensed CCTV installers within Western Australia.

The selection and appointment of a system and designer will comply with the owner's own procurement policy, however, it is recommended that the selection of a designer and installer, particularly for large or complex systems, is undertaken by a panel consisting of people with relevant qualifications and expertise in the equipment that is being considered.

Step 6 – Review and Evaluate

The CCTV system, once installed, should be reviewed and evaluated to ensure that the equipment is meeting the objectives as determined during the planning stage. Indicators of success will depend on the purpose for which the system has been installed and the objectives determined during the planning phase. Positive outcomes may take some time; timeframes should be realistic and actions should be persistent.

A policy review should be initiated following a reasonable implementation period when the degree of applicability and effectiveness of policy and processes can be satisfactorily assessed. The review process may involve internal organisational and external expertise. The information gleaned from this research and analysis can be used to modify the relevant CCTV policy and operational processes. The review process should be a constant method of ensuring that policies and procedures related to the use and management of the CCTV system remain current and effective.

Further Information

Enquiries regarding this document or requests for further information should be directed to:

The Office of Crime Prevention
Western Australia Police
Level 5, 197 St George's Terrace
Perth WA 6000

Ph: (08) 9222 9733
E: crimeprevention@ocp.wa.gov.au
www.crimeprevention.wa.gov.au

5 ADDITIONAL READING

Ditton, J., E. Short, S. Phillips, C. Norris, and G. Armstrong (1999). *The Effect of Closed Circuit Television on Recorded Crime Rates and Public Concern about Crime in Glasgow* (Final report). Edinburgh: The Scottish Office.

Flight, S., Y. v. Heerwaarden, and P. v. Soomeren (2003). "Does CCTV Displace Crime? An Evaluation of the Evidence and a Case Study from Amsterdam." In M. Gill (ed.), CCTV. Leicester: Perpetuity Press.

Gill, M & Spriggs, A. (2005). Assessing the impact of CCTV. Home Office Research Study Number 929. Home Office Research, Development and Statistics Directorate, London.

Scarman Centre National CCTV Evaluation Team (2003). National evaluation of CCTV: early findings on scheme implementation – effective practice guide. Home Office Research, Development and Statistics Directorate, London.

Tilley, N. (1993). Understanding car parks, crime and CCTV: Evaluation lessons from Safer Cities. Police Research Group, Home Office Police Department. London.

Weblinks

www.police.wa.gov.au

www.crimeprevention.wa.gov.au

www.saiwa.com.au

www.asial.asn.net

www.rgl.wa.gov.au

www.saiglobal.com

https://blueiris.police.wa.gov.au

Legislation

Security and Related Activities (Control) Act 1996

Surveillance Devices Act 1998

Acknowledgements

The Office of Crime Prevention wishes to thank and acknowledge the contribution of the following individuals and organisations in the development of this document:

Western Australia Police, Integracom, WA Department of Education, Main Roads WA, WA State CCTV Working Group, WA State Solicitors Office, Arthur Barker, Bosch.

Office of
Crime Prevention

Western Australian Police
Office of Crime Prevention
Level 5, 197 St Georges Terrace
PERTH, WESTERN AUSTRALIA 6000
Telephone: 08 9222 9733
Facsimile: 08 9222 8705
Email: crimeprevention@ocp.wa.gov.au
Website: www.crimeprevention.wa.gov.au

NOVEMBER 2009 • 4146 Design Design