Camera Surveillance

– Test your system before a criminal does.

Guidelines produced by
The Swedish National Laboratory of Forensic Science,
The Swedish Police,
The Swedish Bankers' Association and
The Swedish Federation of Trade and Services

Camera surveillance

–Test your system before a criminal does!

Guidelines produced by

The Swedish National Laboratory of Forensic Science,
The Swedish Police,
The Swedish Bankers' Association and
The Swedish Federation of Trade and Services

Author and contact person
Peter Bergström
Swedish National Laboratory of Forensic Science
581 94 Linköping
Telephone: +46 (0) 13-24 17 25
E-mail peter.bergstrom@skl.police.se

Publisher
Swedish National Laboratory of Forensic Science
581 94 Linköping
www.skl.polisen.se
Telephone: +46 (0) 13-24 14 00 (switchboard)
E-mail skl@skl.police.se

URN:NBN:se-2005-19
www.skl.polisen.se

Linköping 2005

Table of Contents

Foreword iii
1 Introduction 1
1.1 How to use this document 2
2 System levels 3
3 The Public Camera Surveillance Act 5
3.1 Proposed amendment 6
4 Requirements regarding the image material 7
4.1 Image content 7
4.2 Image quality 7
5 Accessibility 9
5.1 Functional requirements regarding the image media and the image format 9
5.2 Functional requirements regarding the media player 10
6 Security 11
6.1 Maintenance 12
7 Documentation 13
Appendix A SKL Test Chart 15
Appendix B Inspection and maintenance schedule 17
Appendix C Incident Checklist 19
Appendix D Glossary 23
References 25

Foreword

Camera surveillance can provide excellent protection against certain types of crime. Unfortunately not all systems can supply pictures of sufficient quality to provide the kind of protection expected by the user.

In order to provide an opportunity for manufacturers, installation engineers, users, authorities and other interested persons to meet and discuss the problems and possible solutions, the Swedish National Laboratory of Forensic Science (SKL) has hosted *Forums for Videosurveillance* conferences on two occasions.

At the first conference, held in September 2003, there were requests for recommendations about how to avoid known problems, as well as guidelines about what would be required to make the pictures useful within the legal system. The result was a number of recommendations and guidelines [3, 4, 5, 6, 7] as well as a survey of the police's capability for handling various image media and formats.

The second conference, in March 2005, agreed to continue the work on developing standards for camera surveillance systems, with a number of requirements divided into three to five system levels. This would be done in two stages. Firstly, the users, represented by the Swedish Bankers' Association, the Swedish Federation of Trade and Services, the Swedish Police and the Swedish National Laboratory of Forensic Science, would produce documentation based on their needs. Once this was done, manufacturers and installation engineers would be given an opportunity to express their views, via their association SweLarm.

This document is the result of the work of the users. The user working committee consisted of Åke Björk, representative of the Swedish Bankers' Association, Dick Malmlund from the Swedish Federation of Trade and Services, Staffan Elm, Jerker Jansson and Michael Franke from the Police and Peter Bergström from the Swedish National Laboratory of Forensic Science. These representatives arranged for a preliminary version of this document to be sent to their respective organisations for comments. Opinions received have been taken into consideration in preparing the present version.

1 Introduction

This document is produced as part of the collaboration between the Swedish Bankers' Association, the Swedish Federation of Trade and Services, the Swedish Police and the Swedish National Laboratory of Forensic Science (SKL), and provides guidelines for camera surveillance systems so that the pictures can be used by the Police and the rest of the legal system, as well as serving in the fight against crime.

As the owner or purchaser of a camera surveillance system, it is important to be aware of the degree of protection the system provides, and whether it corresponds to the security requirements in question. It is thus crucial to establish specifications regarding what should be viewable and where. This may involve being able to recognise the faces of persons passing through an entrance, read the number plate of a vehicle or monitor transactions at a Cashier.

A good method of testing whether a system can fulfil the established specifications is to perform practical tests. Ask someone to perform some action in front of the camera, or park a car in the place under surveillance. This should be done under the same conditions as those for which the system is intended. Then transfer the image material to the system's removable media. Check the pictures from this medium rather than those displayed directly on the screen. What is interesting is the quality of the pictures delivered by the system. Is it possible to see the objects specified in the requirements? If you can't see something, there is generally nothing more that can be done. Or as we say,

- Test your system before a criminal does!

If an incident occurs, we generally want the system to answer these questions: *What actually happened?* and *Who did it?* Wide-angle images must be available to give an impression about the chain of events, while detailed close-ups are needed to make identification possible.

The quality and content of the image material that the system delivers is crucial for reconstructing the chain of events and identifying persons and objects. In addition, secure procedures are needed to avoid challenges to the image material and to protect the integrity of the public.

To increase awareness and security around camera surveillance systems, the Swedish Bankers' Association, the Swedish Federation of Trade and Services, the Swedish Police and the Swedish National Laboratory of Forensic Science have worked together to produce guidelines with specifications for camera surveillance systems. The specifications apply to the *image material* supplied by the system and the *handling* of the image material. The specifications regarding the image material apply to the quality and content of the pictures, while handling concerns accessibility, security and requirements for system documentation.

Based on these specifications, four system levels have been designed.

- Chain of events (A)
- Characteristic features (B)
- Identification (C)
- Biometry (D)

Systems that fulfil the specifications in the first level (A) should be able to supply wide-angle images in the surveillance area. At level 2 (B), the system must also be able to supply close-up images from the most important locations in the surveillance area. At the next level (C), the requirements for these close-ups are raised to enhance the possibility of identification. To further improve the chances of reconstructing the chain of events and identification, the fourth level (D) requires the floor pattern, more camera directions, etc. Regardless of system level, a fundamental requirement of course is that the system complies with the Public Camera Surveillance Act [1].

For more information about guidelines and recommendations for camera surveillance systems, the documents produced by the Swedish Bankers' Association [2, 3], the Swedish Federation of Trade and Services [4], the Swedish Theft Prevention Association [5], the Swedish Police [6] and the Swedish National Laboratory of Forensic Science [7] are recommended. The guidelines issued by the Swedish Bankers' Association and the Swedish Federation of Trade and Services are directed towards the needs of their members, the Swedish Theft Prevention Association's guidelines are directed towards systems monitored by one operator, the Swedish Police guidelines contain ten important points to increase the solution of crimes, and the recommendations of the Swedish National Laboratory of Forensic Science give more information about what is required by the system and tips for success.

1.1 How to use this document

The core of this document is Table 1 on page 3. The table shows a number of specifications for camera surveillance systems, divided into 4 system levels.

The content of Table 1 is then explained in the sections that follow. In the text, the word *shall* is used in connection with the basic requirements in system level A, while the word *should* is used for other requirements. In addition, there are some *recommendations* that are beyond the requirements of the system levels shown in Table 1. The recommendations are therefore not requirements; the recommendations are simply to help achieve the requirements, but other solutions may be available.

2 System levels

The four system levels are primarily defined by the quality and content of the final image material. There are also requirements for allowing rapid and complete accessibility to the image material, security relating to the image material, and access to more detailed information about the camera surveillance system if this is required.

The following table shows what is required at the different levels. The different requirements are then described in the chapters that follow.

Requirements			System level				Ch.
			A	B	C	D	
Position			x	x	x	x	3
Image quality	Chain of events		x	x	x	x	4.2
	Characteristic features			x	x	x	
	Identification				x	x	
Image content	Chain of events		x	x	x	x	4.1
	Full-length image			x	x	x	
	Mid close-up image				x	x	
	Biometry information					x	
Accessibility	Image media	VHS or CD-R	x	x	x	x	5.1
		also other standard formats		x	x	x	
	Media player	Accompanies the image material	x	x	x	x	5.2
		Distinguishes between the cameras	x	x	x	x	
		Plays image by image	x	x	x	x	
		Exports still pictures	x	x	x	x	
		Exports sequences of still pictures		x	x	x	
	Picture format	Standard format	x	x	x	x	5.1
		Sequential format		x	x	x	
		Frame format			x	x	
Security	Origin	Time and date stamping	x	x	x	x	6
		Signed for at transfer of image material	x	x	x	x	
	Operational security	Locked in	x	x	x	x	
		Trained personnel	x	x	x	x	
		Vandalisation protection	x	x	x	x	
		Logbook		x	x	x	
		Protection against power surges		x	x	x	
		Safe deactivation during power cuts			x	x	
		UPS				x	
	Maintenance	Service	x	x	x	x	
		Inspection (weekly)	x	x	x	x	
		Inspection (daily)			x	x	
Document	By the recording equipment	Incident checklist	x	x	x	x	7
		System description supplied with the image material	x	x	x	x	
		Test pictures		x	x	x	
	On request	Technical description				x	

Table 1. Requirements at the four system levels.

3 The Public Camera Surveillance Act

Camera surveillance is regulated in the *Public Camera Surveillance Act (1998:150)* and the *Public Camera Surveillance Ordinance (1998:314)* [3]. The County Administrative Board grants licences and exercises supervision. Camera surveillance is only allowed if the purpose is to deter crime, detect crime and, if a crime occurs, to establish the chain of events and identities of people.

A *licence* is needed for surveillance of a public place. Strictly private areas, such as residences, gardens, staircases in blocks of flats, or areas of a workplace to which the public does not have access, do not require a licence.

Camera surveillance in bank premises, post offices, and near ATM adjacent to such premises, is exempted from the licence requirement. Exemption also applies to shops, but under certain conditions. For these places, a *notification* of the surveillance to the County Administrative Board is sufficient. One condition for this is that the cameras are in a fixed position and have fixed optics. In order for a notification to suffice for surveillance in a shop, an agreement is required with a trade organisation that represents the employees. Furthermore, only pictures from the till area and entrances may be recorded. For other parts of the shop where customers have access, a licence is required if the cameras are to be connected to recording equipment.

Regardless of where the camera surveillance takes place, *information* must be provided that the area is under surveillance, through clear signs in the surveillance area. Where premises are under surveillance, signs should be on display at each entrance.

Figure 1 illustrates two examples of where the different regulations for camera surveillance apply.

The Public Camera Surveillance Act also covers the *recording of sound* in connection with surveillance. Listening or recording of sound requires a licence, and may not be conducted without providing information. Banks and post offices are exempt from the requirement for a licence when the system is activated on suspicion of a crime (alarm mode).

Certain authorities, such as the police, are entitled to carry out surveillance without a licence in certain cases.

Image and audio material may be *stored* for up to one month, unless a special licence has been granted. The police and courts are entitled to store material for longer if it comprises part of an investigation of a crime.

Only authorised persons shall have access to recording equipment and recorded material. It is important that the authenticity of recorded image material can be guaranteed. An authorised person is one that needs access to keep the system operating. Recorded material may only be reviewed on suspicion of a crime, and then by a security manager or the police. Anyone authorised to access image or audio material is obliged to observe secrecy pursuant to the provisions in the Secrecy Act (1980:100).

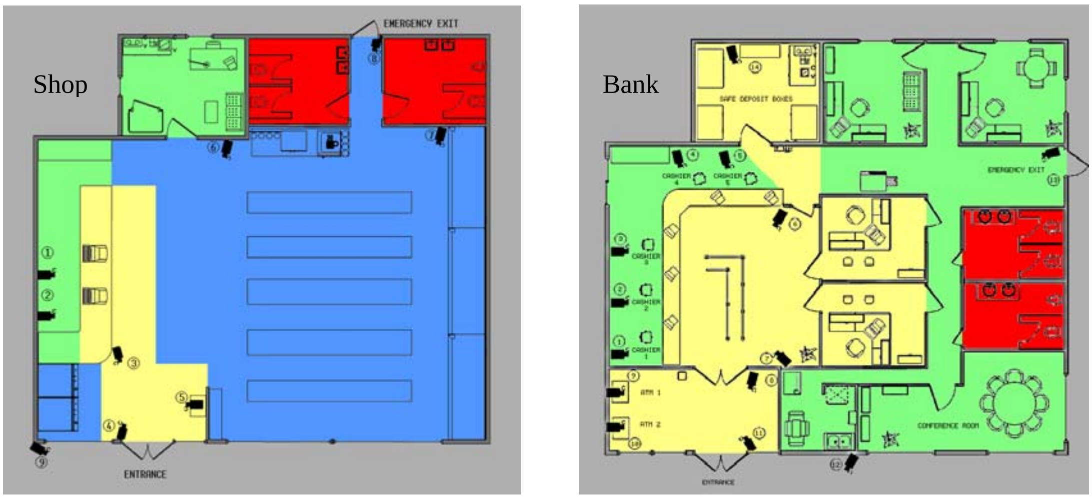


Figure 1. Examples of a shop premises (left) and a bank premises (right). The different colours show the areas for which different regulations for camera surveillance apply.

Green	Staff area	Clear signs
Yellow	Customer area	Notification to County Administrative Board (CAB)
Blue	Customer area	Notification to CAB if the camera is connected to a screen Licence from CAB if the camera is connected to recording equipment
Grey	Outdoors	Licence from CAB
Red	Toilet/Fitting cubicle	Not permitted

3.1 *Proposed amendments*

A proposal to amend the Act is being worked on. The new proposal extends the surveillance area in shops for which a notification to the County Administrative Board is sufficient. The proposal also obliges the suppliers of camera surveillance systems to provide information to the customer about the Act.

4 Requirements regarding the image material

Using the image material, what we usually want to know is: *What happened?* and *Who/What is on the images?* The most important factors that determine whether the image material can give the desired information are the system's field of view and the quality of the images. The field of view is crucial for using the images to track a chain of events, while the image quality determines whether or not people and objects can be identified.

Capturing both wide-angle and close-up images using the same camera is virtually impossible. A camera surveillance system should therefore have two types of cameras – wide-angle cameras and close-up cameras.

The requirements discussed in this document refer to the image material supplied by the system. However, for successful images, it is important to consider lighting, camera placement, concealed cameras, recording media, compressing, changed image frequency during movement detection and alarms, and that each camera just has one task.

4.1 Image content

The system should primarily make it possible to convey an impression of the *chain of events*. This means that the wide-angle images can verify a witness's statement, provide information about where clues can be found, and possibly allow a witness to recognise a person or an object.

Using close-up images increases the possibility of identifying people and objects. Close-ups with *full-length images* can give an impression of clothes, posture, objects carried and, in combination with a height marker in an image, an estimation of the person's height. Images of *mid close-up size* are required in order to produce a really good image quality.

If an object rather than a person is to be monitored, a full-length image covers the entire object while a mid close-up shows the most important feature. For example, if the aim is to identify a car, a full-length image provides information about colour, make and model, while the mid close-up will make it possible to read the number plate.

In order to give a more accurate reconstruction of a chain of events, to give precise information about where to look for footprints, and to allow a better estimation of a person's height and other body measurements, we need to know where the person placed his/her feet. This is simplified if the wide-angle and full-length images show a squared pattern on the floor. In addition, measurements of height require fixed vertical lines showing heights. If the probable walking route and the most vulnerable places, such as the Cashiers, are also filmed from several directions[1], this makes it more possible to measure height, movement patterns and other *biometrical information*.

4.2 Image quality

The requirements for image quality are divided into three levels: chain of events, characteristic features and identification.

[1] The cameras should be synchronised so that the pictures are taken simultaneously.

What is required to give an impression of the *chain of events* depends on the type of events that the system is to register. Is it sufficient to be able to confirm that someone has been present in the area, or is more information required from the wide-angle images? The police request that the wide-angle images make it possible to form an impression of what a person is holding, such as a gun or some other object.

Based on this level of reproduction of detail in a wide-angle image, and what is normally required for the Swedish National Laboratory of Forensic Science (SKL) to comment on *characteristic features* or *identify* a suspect, SKL has produced a test chart with associated requirements [7]. The test chart is a modified version of an optician's eye chart (see Figure 2). Placing the chart in the camera's main surveillance area, and seeing which row can be read in the image material, gives an impression of the system's ability to reproduce detail. Appendix A shows the chart in actual size, and a description of how the chart is intended to be used.

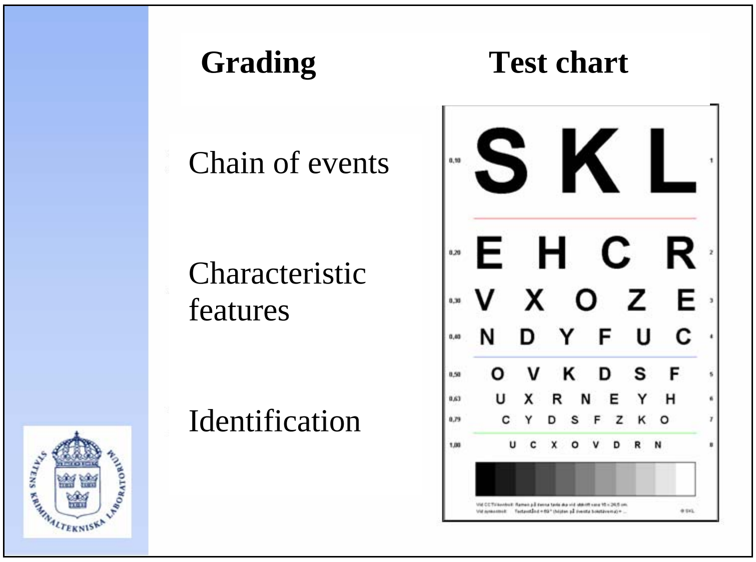


Figure 2. The SKL test chart (in reduced scale)

Table 2 indicates which row should be readable and what image speed is required for wide-angle images and the different levels of close-ups. The requirement for image speed applies when the incident is taking place, but is then a minimum requirement.

Picture type	Readable row on test chart	Picture speed [frames/s]
Chain of events	1	1
Characteristic features	2-5	3
Identification	6-8	5
Biometry	2-5	5

Table 2. Requirements for picture quality.

For a reasonable system today, an image size of 1-1.5 full-length figures corresponds to the requirement for the *Chain of events* level, 1-0.5 half-length figures for *Characteristic features*, and mid close-up size for *Identification*.

5 Accessibility

When an incident occurs, the image material must be quickly and easily accessible for the people concerned, including the police. This involves a number of requirements: the removal from the recording equipment, the recipient must be able to handle the image material, the recipient must have access to the necessary media player, and the media player must function satisfactorily.

5.1 Functional requirements regarding the media and the format

The requirements for image media primarily concern rapid and simple handling. The police and other authorities are unable to handle all types of image media. Different police districts have invested in different types of equipment because of the wide range available. However, every district can handle VHS tapes and CDs locally. Furthermore, measures are being taken to enable them to handle DVDs and removable hard drives with USB connections and compatible with NTFS. Other standard formats can also be handled, but not always locally, which can cause delays in a case.

Previously, the image format was linked to the image media, but this is not the case for computer-related media. *The basic requirement for image format is that it must be a standard format*. This means the police have a greater chance of being able to handle the format. This also increases familiarity with the format, and thereby reliability in legal proceedings.

Image format is often divided into still picture format, sequential picture format and video format. In a sequential format, each image is treated individually while, in a video format, the similarity between adjacent images in a sequence of images is used when compressing. In a video format such as MPEG, the amount of detail is reduced, especially in the moving parts of the image. This is acceptable in an entertainment film but is unsuitable for camera surveillance images because it is usually the moving parts of the image that are most interesting, such as a suspect. Consequently, image material from surveillance cameras should be stored in still picture format or sequential picture format.

In many sequential image formats and video formats, the frame is divided up into two fields. If only one field is saved, the vertical resolution is halved. To improve the chances of identification, the pictures should be saved in frame format.

TIFF and JPEG2000 (in lossless mode) are recommended as lossless compression formats. JPEG and JPEG2000 are recommended as lossy compression formats. JPEG and TIFF are the most commonly used still picture formats used today, and they are supported by the National Archives, which facilitates police archiving. JPEG2000 is a relatively new format with many advantages:

- JPEG2000 usually gives better visual images at a given level of compression than any other standard method.
- The same algorithm can give both lossy and lossless compression.
- JPEG2000 is available in a standardised sequential version, M-JPEG2000.

- JPEG2000 offers several interesting functionalities, such as region of interest coding.

5.2 Functional requirements regarding the media player

If the most common standard formats are not used, it is up to the system user to ensure that an associated media player and codec are also supplied with the supplied image material in the event of an incident.

The media player must be able to:

- Distinguish between and play each camera individually
- Rapidly come to the sequence in question
- Show the images in full resolution
- Play image by image (forwards and backwards)
- Export still pictures [2]
- Manage sound (if it is stored)

In addition, the player should be able to:

- Export sequences of still pictures
- Provide information about resolution, colour format, compression method, image frequency, storage format, etc.
- Zoom (without interpolation)
- Change playing speed
- Show the image in field format if the recording has been made in this format.

For rapid and simple police handling, the media player should be able to:

- Be installed and run under Windows XP
- Completely uninstall.
- Export still pictures in the JPEG or TIFF picture formats.

[2] These are the images that are to satisfy the requirements for image quality. Avoid therefore converting the format of the images, because this always means loss of information.

6 Security

Security around the image material concerns physical security and person-related security issues. The physical security is about the storage of image media and equipment, and the system's operational reliability. The person-related security matters involve training of staff, authorisation, the keeping of a logbook, and secure procedures during the transfer of image material.

The security requirements are largely the same regardless of the system level. The basic requirements are as follows:

- A camera surveillance system must record text information such as time, date, and preferably also the camera ID (identity) together with the images. The clock should be synchronised against an external source for automatic setting [3].
- Image media and recording equipment must be kept in a locked area. This area must have no signs or indicate its contents in any other way to unauthorised persons.
- The power switch must be in a locked area, or the equipment must be permanently connected.
- The staff must be trained in handling the equipment, and be given information about the Public Camera Surveillance Act.
- Vandalisation protection. Make it difficult for the criminal to cover, break or redirect the cameras. If possible, use hidden cameras, misleading imitations, etc. In high-risk areas, such as bank safety deposit boxes and security rooms, the door should automatically lock if the cameras in question are put out of action.
- In the event of an incident, the system time should be checked against the Speaking Clock.
- Image material must be transferred on read-only image media.
- When image material is transferred, a document must be produced to show the person who has given out the material and who the recipient is, the content of the image material and a brief description about what has happened. Both parties then sign this document. Place the image material in a deposit bag, which is labelled and signed for. The purpose of these measures is to ensure traceability and the authenticity of the material. (Appendix C contains an example of such a document.)

To further increase the security, the system should be designed so that it automatically switches off when there is a power cut, and then starts up again when the power is restored. This must happen without putting recorded material at risk. Furthermore, the system should be secured against power surges in the electricity network. The next step is to equip the system with UPS (Uninterruptible Power Supply). It must never pay to carry out criminal activities during a power cut, or to deliberately cause a power cut.

To enhance the security around the management of the system, a logbook should be kept in which maintenance and inspection measures are detailed and signed, with information about the date/time and the name of the person carrying out the measures.

[3] Synchronise the clocks for all the security systems against each other, such as the camera surveillance system, burglar alarms, cashier systems, passage systems, etc..

When an application is made to the County Administrative Board for a licence for camera surveillance, a request should be made to keep the technical information about the system confidential. This is especially important if the system uses camouflaged or hidden cameras.

6.1 Maintenance

A system must be maintained if it is to function satisfactorily. This means that the system is regularly checked and complies with the manufacturer’s service recommendations. If faults are discovered, these should be remedied as soon as possible. Everything that is done to the system (inspections, maintenance, upgrades, etc.) should also be recorded and signed in a logbook.

The basic requirement is that the manufacturer’s service recommendations are followed. Furthermore, there must be a schedule for regular checks of correct operation. A simple inspection should be done every day, while a somewhat more detailed inspection should be carried out every month. Appendix B includes a proposal for an inspection and maintenance schedule.

If the system is changed, this must be documented, and the documents concerned must be updated. Any changes in the area under surveillance, such as changes in lighting, rearrangement of furniture, screens, etc. can have a major impact on the existing camera surveillance. Camera placement, area of coverage and lighting should be reviewed before making any changes in the premises or moving furniture.

7 Documentation

The owner of a surveillance system must keep system documentation by the recording equipment. The documentation must include the following:

- *Incident checklist* of what to do.
  - Contact the police
  - Check the system time with the Speaking Clock
  - Save all stored image material
  - Ensure the removable media is read-only
  - Label the image media (name of institution, date and time of the incident)
  - Ensure the security of the image media - place it in a deposit bag, store in a locked place until it is transferred, avoid playing original tapes, avoid environmental impact, such as heat, moisture, sunlight and magnetic fields
  - Recipient should sign when the image medium is handed over
  - Check that the recipient can review the image media and the image format – if not, remedy
- *System description* that is supplied together with the image material.
  - Number of cameras
  - Plan of the premises showing camera placement[4] and fixed furniture
  - Contact persons at the user and the system installation company (name, telephone numbers, companies)
  - Information about image format, audio format and media player
- Manual containing a description of how to transfer the image material to a removable medium. It must be easy to understand so that all authorised persons can follow the instructions.

In addition there should be the following:

- User-friendly manual.
- Test images from each camera with a person and possibly a test chart. This is excellent documentation for checking that camera direction, picture quality, etc. is maintained.
- Technical description. A list with serial numbers of all system components such as cameras, optical devices, muliplexer/switch, recording equipment, etc. For digital systems, this list must also include software (name, version, any settings) and hardware.
- Logbook/operational journal in which all checks, maintenance, faults, etc. are recorded.

Appendix C contains an example of an incident checklist and a plan of the premises.

[4] Supplement with an image from each camera, labelled with camera number and description of placement.

APPENDIX A SKL Test Chart

The purpose of the Swedish National Laboratory of Forensic Science (SKL) test chart is to indicate the image quality required by a CCTV system in relation to the needs of the police.

Procedure:

1) Print out the test chart. It is shown on a scale of 1:1 on the next page. In the printed version, the frame around the chart must be 16 x 24.5 cm.
2) Place the chart in the position where the image quality is to be measured. A person should stand beside the chart.
3) Then check in the image material that the system supplies which row on the chart can be read. A row is regarded as readable if more than 60 % of the letters can be correctly read. However, caution should be exercised if the same reviewer looks at several test images using the same test chart, because the reviewer soon learns the combinations of letters.
4) Check in the following table the expected use of these images.

Picture type	Readable row on test chart	Picture speed [whole pictures/s]
Chain of events	1	1
Characteristic features	2-5	3
Identification	6-8	5
Biometry	2-5	5

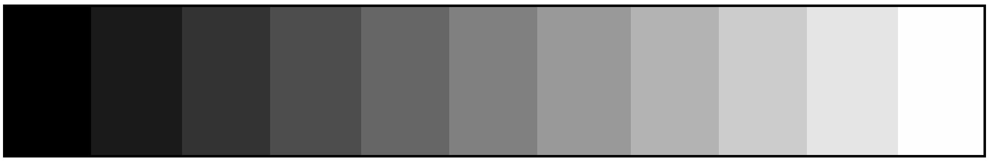
Table 3. Requirements for image quality.

The images from a wide-angle camera must allow the image material to be used to form an impression of the *chain of events*. This can be done at different levels. Here, the level is set so that the image quality makes it possible to determine the type of object a person is holding, such as a bag or a gun. For this to be possible, row 1 of the test chart should be readable in the camera's main area of surveillance.

If the limit for what can be read is row 2, 3 or 4, the image material may be used to describe a person's facial shape and *characteristic features*. The higher the row number that is readable, the greater the probability.

If rows 5, 6 or 7 can be read, it is probable that a suspected person can be *identified*. Again, the higher the row number that is readable, the greater the probability. For identification, it should also be possible to differentiate between most of the grey scale levels on the test chart.

0.10	S K L	1
0.20	E H C R	2
0.30	V X O Z E	3
0.40	N D Y F U C	4
0.50	O V K D S F	5
0.63	U X R N E Y H	6
0.79	C Y D S F Z K O	7
1.00	U C X O V D R N	8



CCTV check: When printed out, the frame of this board is to be 16 x 24.5 cm.

Vision check: Test distance = 69 * (height of the topmost letters) = ... © SKL

APPENDIX B Inspection and maintenance schedule

The following is a proposal for an inspection and maintenance schedule. If the manufacturers have any other recommendations, naturally these must be followed.

	Activity	Action
Daily	Are all cameras working, correctly aimed, and do they focus on the correct place?	View live images on the screen for each camera, e.g. using a field
	Check that nothing prevents the camera's view.	Remove objects that are inappropriately placed in the image.
	Is the recording working?	Is the tape running?
	Is the date and time correct?	Check feasibility.
	Is it time to change the videotape?	Archive the one removed and insert a new one.
	Is the system secured?	Check that cupboards and doors are locked.
Monthly	Clean the camera lenses.	Follow the manufacturers' recommendations.
	Check the environment for the equipment.	Compare temperature, air humidity, etc. with the manufacturers' recommendations.
	Is the date and time correct?	Ring the Speaking Clock.
	Is the recording working ok?	Rewind the recording 30s and check for new recording.
Annually	Does the system still provide the desired image quality?	Check with test images taken when the system was installed.
	Check the cameras' white balance.	Follow the camera manuals.
	If a hard drive is used, check its status.	Follow the manufacturers' recommendations.
	Check that all documents are in order.	Replace lost, damaged or outdated documents.
	Check that all relevant staff are familiar with the system.	Ensure that staff practice.
	Check correct transfer of image material to removable media.	Make a test recording and then review it on another piece of equipment .
	Clean the recording equipment.	Follow the manufacturers' recommendations.

Table 4. Inspection and maintenance schedule.

APPENDIX C Incident Checklist

- **Contact the police**.

  Date/time of the incident: ______________________________

  Brief description: ______________________________

  ____

  ____

- **Check time/date on recording equipment** with the Speaking Clock and record deviations.

  Date/time according to the system: ______________________________

  Deviation compared with Speaking Clock: ______________________________

- **Save all stored image material and transfer it to removable medium** without lowering the quality. If possible, make two copies, one original and a backup copy.

- **Make the removable medium read-only** to prevent recording over the material. On VHS tapes, break the plastic tongue on the reverse of the cassette. For disks, use CD-R or DVD-R disks.

- **Label the removable medium** with the name of the institution, date and time of the incident. The person doing this should also sign the medium.

- **Secure the image medium.**
  - If possible place the image medium in a labelled deposit bag. Seal and sign the bag.
  - *Lock in the image medium* if it is not transferred directly.
  - *Avoid playing videotapes.* Every time videotapes are played, the image quality deteriorates. A copied version should be used for reviewing. The original should be played a minimal number of times.
  - *Avoid environmental impact.* Tapes should not come close to magnetic fields, such as near a TV, radio or loudspeakers. Tapes and disks must not be subjected to heat, excessive moisture or direct sunlight.

- **Check that the police can manage the image material optimally.** If not, ensure that the necessary hardware and software, with the appropriate image-processing program, are sent with the images.

- Ensure that the necessary **documentation** is available.
  - *Contact persons:* Institution Installation company

    Name: ____________________ ____________________

    Telephone: ____________________ ____________________

    E-mail: ____________________ ____________________
  - *Number of cameras:* ____________________
  - *Image format:* ____________________
  - *Audio format (where app):* ____________________
  - *Plan of building* showing camera placement and fixed furniture (preferably test images from each camera).
  - Any technical description

Signatures: Date Name Institution/Authority

Issuer: __________ ____________________ ____________________

Recipient: __________ ____________________ ____________________

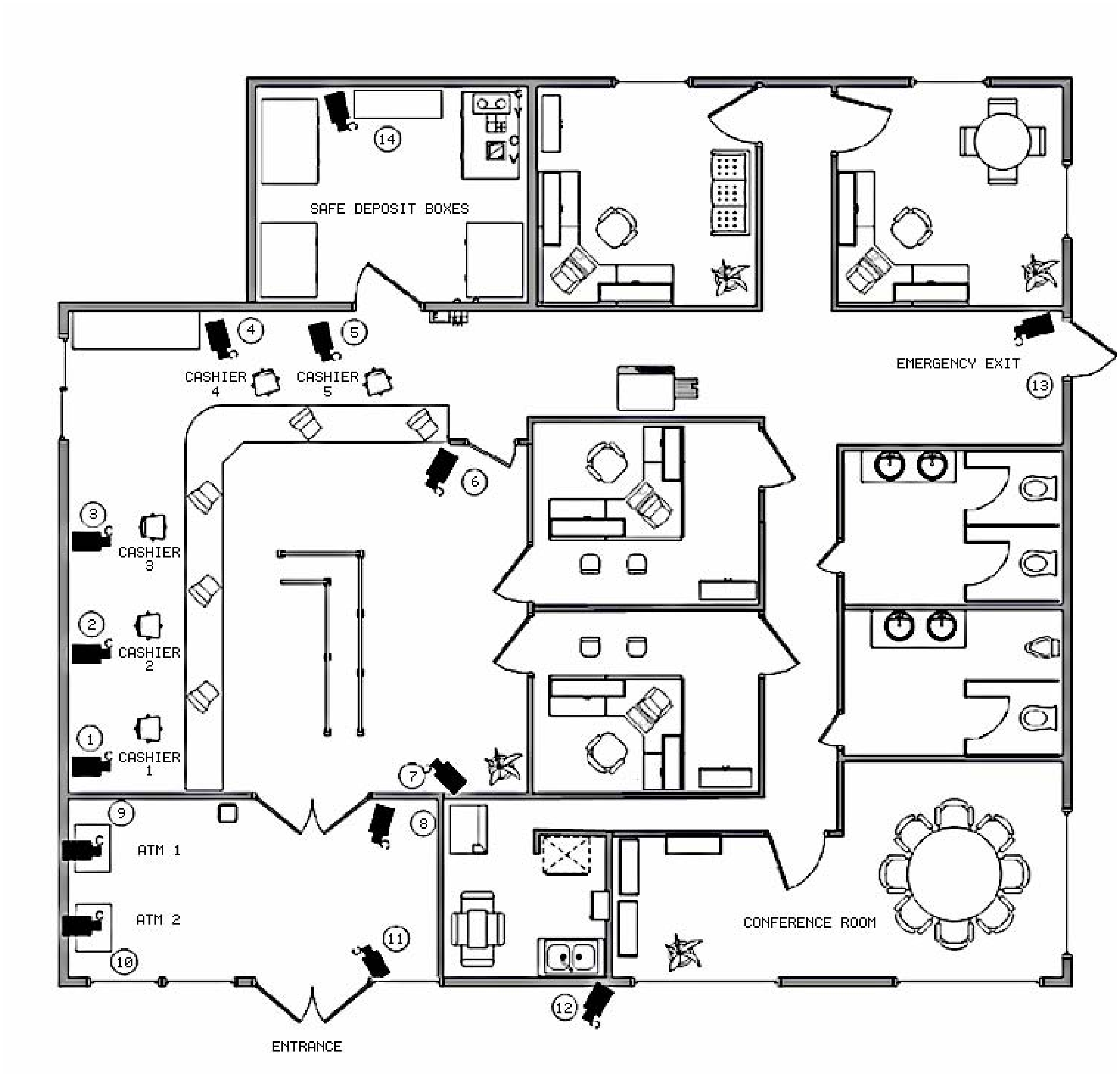


Figure 3. Example of camera placements in a bank.

Camera number:

1.	Cashier	(C)
2.	Cashier	(C)
3.	Cashier	(C)
4.	Cashier	(C)
5.	Cashier	(C)
6.	Customer area	(W)
7.	Customer area	(W)
8.	Entrance	(C)
9.	ATM	(C)
10.	ATM	(C)
11.	Entrance	(C)
12.	Outside the entrance	(W)
13.	Emergency exit	(C)
14.	Safety deposit boxes	(C)

C = Close-up camera
W = Wide-angle camera

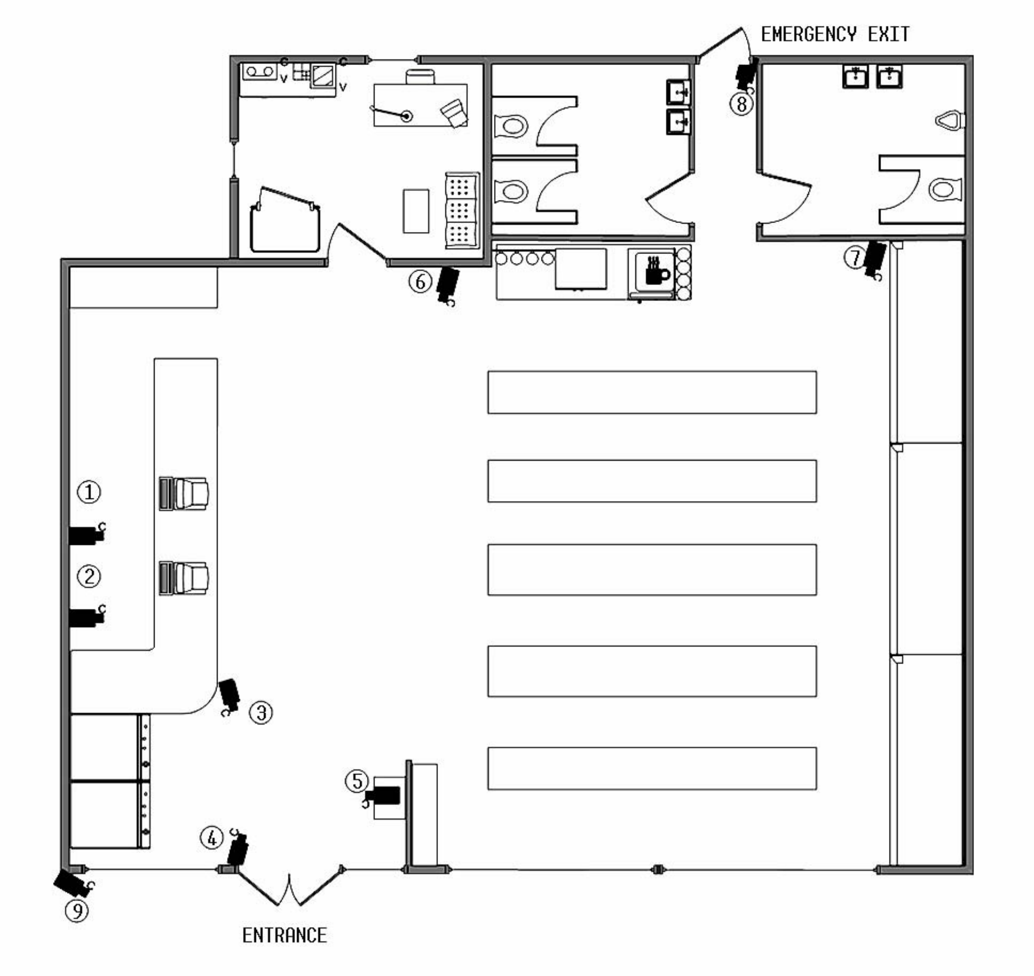


Figure 4. Example of camera placements in a shop.

Camera number:

1.	Cashier	(C)	7.	Customer area	(W)
2.	Cashier	(C)	8.	Emergency exit	(C)
3.	Entrance	(C)	9.	Outside the entrance	(W)
4.	Entrance	(C)			
5.	ATM	(C)	C	= Close-up camera	
6.	Customer area	(W)	W	= Wide-angle camera	

APPENDIX D Glossary

Characteristic features	This can be shape, proportions, colour, etc. Information that gives certain indications but is not sufficient for identification.
Image medium	Carrier of image and audio information, e.g. VHS tapes, CD-R and DVD-R disks and hard drives.
Codec	Codec is an acronym for encoder-decoder. A video codec consists of a program library that contains a program code for compressing and decompressing. It can also cover other treatments of audio and image information, such as synchronisation.
Chain of events	A sequence of events that follow a chronological order.
Identification	Establishment of a person or object’s identity based on individual characteristics.
Incident	An event that the camera surveillance system is intended to capture with images, possibly with sound.
Institution	In this document, institution refers to the user/owner of the camera surveillance system, i.e. the bank, shop or other user.
Supplied image material	The image material that the police or other recipients receive.
NTFS	New Technology File System.
Close-up camera	Camera intended for recording detailed close-up pictures.
Area of coverage	Area within which a camera can record images of a desired quality.
UPS	Uninterruptible Power Supply. Ensures power supply using an auxiliary source.
Wide-angle camera	Camera intended for recording a chain of events.

References

[1] *Public Camera Surveillance Act (1998:150).* www.riksdagen.se/debatt/sfst/index.asp

[2] Swedish Bankers' Association, *Norm för bank CCTV-anläggning*, 2000.

[3] Swedish Bankers' Association, *Norm för bank CCTV-anläggning Tillägg Digitala system med lagring*, 2003.

[4] Swedish Federation of Trade and Services, *Övervakningskameror*, 2004.

[5] Swelarm and Swedish Theft Prevention Association, *CCTV Kameraövervakning – utan krusiduller*, ISBN 91-89234-25-1, 2004.

[6] Police Guidelines, 2005.

[7] Swedish National Laboratory of Forensic Science, *Rekommendationer vid användande av Kameraövervakningssystem*, ISBN 91-89110-25-0, 2005.

Guidelines about camera surveillance systems. Produced by the Swedish National Laboratory of Forensic Science, the Swedish Police, the Swedish Bankers' Association and the Swedish Federation of Trade and Services.

Guidelines about camera surveillance systems.
Produced by the Swedish National Laboratory of Forensic Science, the Swedish Police, the Swedish Bankers' Association and the Swedish Federation of Trade and Services.