



**SURVEILLANCE CAMERA
COMMISSIONER**

PASSPORT TO COMPLIANCE

STAGE 3

IMPLEMENTATION

3.1 Project management

Given the complexity of the project, it is strongly recommended that you pull together a working group for the management of the project, comprising representatives of all of all key stakeholders. This group, often referred to as the “Project Board”, will be responsible for ensuring that the project delivers on time and within budget. One person should be the overall project leader, responsible for delivering the project.

For smaller schemes and/or where only a small number of cameras are required you may not need to adopt such a structure. However, even for such small schemes, it is important that you manage the project carefully to ensure that the system comes on stream on time and in budget.

There are numerous text books and guides in relation to project management and it is not proposed to go through project management in detail here. However, this guidance will signpost you to some useful project management material.

However, at the heart of any effective project management process is a clear project plan. As a minimum this should:

- List all of the tasks and key stages of the work
- Show the start and completion dates for each task
- Show what resources are needed for each task and who is responsible for delivering that task
- Include a risk register that highlights the risks to task and project delivery as they emerge
- This will enable prompt corrective action to be taken to minimise or even remove the risk

It is important that the project plan is updated and reviewed regularly to ensure tight control of the project as it proceeds. You may use a table, such as the one below, which demonstrates how you might plan the tendering process, to help this process.

Task ID	Task name	Duration	Start	Finish	Task Lead
1	Write tender	5 days	5/9/16	12/9/16	Contract services
2	Issue tender	1 day	12/9/16	19/9/16	Contract services
3	Tender return		19/9/16	17/10/16	Contract services
4	Evaluate tenders	3 days	17/10/16	31/10/16	Project Board
5	Decision re contractor	1 day	31/10/16	7/11/16	Project Board
6	Prepare and issue contract	5 days	7/11/16	21/11/16	Contract services

To demonstrate how this works, using the example of issuing the tender, the table states that this will take one day to do, and that it should happen sometime between the 12th and 19th of September. Contract services department will be responsible for carrying this out.

The benefit of this type of approach is that it assigns responsibility for the delivery of the task. Additional tasks can easily be added, or sub-tasks added under the main task headings.

Another useful method of presenting a project plan is Gantt charts. The example below shows that in a Gantt chart:

- All the tasks for the project are shown down the left hand side
- The duration, start and finish dates for each task are also shown in text down the left hand side
- The start date for each task and how long each is expected to take is shown by the bars on the calendar
- The names by the side of the tasks show who is responsible for completing them

Using the tendering example again, week 1 of the project is the start of the project, the week commencing 5th September

Task ID	Task name	Lead	1	2	3	4	5	6	7	8	9	10	11
1	Write tender	CS	■										
2	Issue tender	CS		■									
3	Tender return	CS			■	■	■	■					
4	Evaluate tenders	PB							■	■			
5	Decision re contractor	PB									■		
6	Prepare and issue contract	CS										■	■

As you can see, a Gantt chart is basically a calendar so you could create one manually on a wallchart or in a spreadsheet.

There are a number of methods you can use for effectively managing complex projects. One of these is called PRINCE (PProjects IN Controlled Environments) and though it was developed to manage large information technology projects, over the years it has increasingly been used to manage major programmes, particularly in the public sector, for example the implementation of problem oriented policing in a number of police forces.

The advantage of methods like PRINCE is that they make it possible to keep tight control over projects, particularly where such projects are complex. They are, however, often time consuming to set up and maintain and so are best used for large and complex projects.

There are many other methods that you can use to help to manage projects and you can even buy special project planning software.

It is highly likely that your organisation uses a particular project management methodology or project management software. You should identify the department responsible for managing projects in your organisation and seek their advice. They should be able to assist you in preparing a project plan and may even take responsibility for it.

If you would like to find out more about project management, as a start point, the Local Government Association, has an excellent guide for project managers, which broadly follows the PRINCE methodology and this can be found at <http://www.idea.gov.uk/idk/aio/6056049>.

3.2 Tendering

3.2.1 Writing the tender

It is very likely that in your organisation, there is a department responsible for preparing tenders for work or services. In the first instance you should approach this department and seek their advice regarding preparing the tender. They may even write the tender for you. However, even if this is the case, it is useful to know what a tender should include as this can assist you in your discussions with the tender preparation specialists in your organisation.

A common tender framework for items to be procured or for the delivery of services, is likely to include the following sections, as a minimum.

- Introduction – reason for the tender notice
- Requirement – detailed specification of the work and/or services that are required. This is often in an appendix. In relation to a CCTV system this will be built around the technical specification
- The tender response – what it is you want tenderers to include in their tender. This will usually require tenderers to provide the following:
 - Service proposals – details of how the goods and services outlined in the specification will be delivered.
 - Delivery plan – details of a programme, or project plan, for the delivery of the goods and services proposed

- Quality plan – details of how the delivery of the goods or services will be managed to ensure that required standards are met
- Business continuity plan – contingency arrangements to ensure continuity of service
- Certificate of Bona Fide Tender – signed and dated, this confirms that the details included in the tender are legitimate and that the organisation is authorised to deliver the outlined goods and services
- Environmental statements – details of environmental policies and procedures
- Equal opportunities statements – details of policies and procedures
- CV's of key personnel
- Payment terms – the terms that you will include in the contract, for example, within 30 days of the receipt of a satisfactory invoice
- General instructions
 - Contact point for the organisation issuing the tender, including arrangements for any queries with any questions that tendering organisations might have
 - Date and time deadline for tender submission
 - Method of tender submission
 - Indicative budget – some organisations will provide a range for the amount that they expect the specified goods or services to cost, e.g. in the region of £75,000 to £100,000. Not all organisations do this however
 - Arrangements if the tender is modified
- Evaluation criteria – it is common for the organisation issuing the tender to describe how it intends to evaluate the tender. This is discussed further in section 3.2.3 below
- Contract conditions – it is common for organisations issuing tenders to include a copy of standard contract terms and conditions
- Copyright arrangements – if copyright is a potential issue, the tender should include details of how this should be considered in the tender

3.2.2 EU thresholds and tendering regulations

It is likely that your organisation will have particular tendering regulations that govern how it carries out tendering exercises. In addition, there is a range of European Union regulations regarding how tenders should be publicised across the EU area, according to the potential financial value of tenders.

As noted, it is likely that your organisation will have a department responsible for the preparation of tenders and the management of the tendering process. You should consult with them in the first instance regarding regulations.

Remember if more than one organisation is involved in funding the proposed system, they may have differing tendering regulations. There will need to be agreement regarding which organisation will lead (and hence whose regulations will apply to) the tendering exercise.

3.2.3 Evaluating tenders

As noted above, tenders should state those criteria that you will be using to assess the tender submissions in the tender documents. This is to ensure that tenderers are aware of how their submission will be judged.

Common criteria used in the evaluation of tenders are:

- The extent to which tenderers understand the requirement
- The extent to which proposal meet or “fit” the requirement
- Price
- Cost effectiveness

- Business continuity
- Experience, knowledge and expertise of the organisation and key personnel in carrying out similar work
- Innovative proposals
- Whether risks to project completion have been identified and suitable contingency arrangements outlined

The project board should discuss and agree the criteria that will be used to assess the tender responses.

In order to assist in the decision making process, it is also possible to assess the extent to which tender responses meet the criteria. For example, for each criterion you may consider whether or not their proposals:

- Are significantly less than the minimum requirement – score 1 point
- Just miss the minimum requirement – score 2 points
- Meet the minimum requirement – score 3 points
- Exceeds the minimum requirements – score 4 points

You may also wish to “weight” the criteria i.e. giving greater emphasis to some criteria than others according to their importance to you. For example, you may decide that “the extent to which the proposal meets the requirement” is the most important criterion. As a result, you may decide that the scores for that criterion should be weighted by a factor of 3 (i.e. the scores for this should be multiplied by 3).

As a result, the scores for proposals in relation to that criterion will be:

- Are significantly less than the minimum requirement – score 3 points
- Just miss the minimum requirement – score 6 points
- Meet the minimum requirement – score 9 points
- Exceeds the minimum requirements – score 12 points

By evaluating each proposal against the criteria and scoring them, you should be able to identify the preferred proposal.

Once again, the project board should discuss and agree the scoring for the criteria that will be used to assess the tender responses, whether weighting should be applied to any criteria and what that “weight” should be.

The arrangements for the evaluation of the tender submissions also need to be planned i.e. who, when etc.

In addition to the above, you can carry out some basic checks on a potential contractor to give you the confidence that they are capable of providing the necessary information on the size of CCTV system you want. This could be particularly useful when compiling a list of organisations that you might invite to tender. Factors that you may wish to consider will include:

- Past Contract experience – for example, you may require any potential contractor to be able to demonstrate experience in at least two similar projects. You may ask them to provide contact details of those with whom they have previously worked, for reference purposes
- Their knowledge of the appropriate standards i.e. BS 62676 series, BS 8418)
- For a security company, you need to know that the company has the resources to meet your needs i.e. how many engineers, 24/7 cover (depending on contract), vehicles, spares
- Whether its employees who have access to your proposed CCTV system or your premises, are security vetted.

- Whether the security company is inspected by an inspectorate accredited by the United Kingdom Accreditation Service (<http://www.ukas.com>) which have the scope for CCTV systems or CCTV monitoring, for example:
 - National Security Inspectorate (<http://www.nsi.org.uk>)
 - SSAIB (<http://ssaib.org/>)
 - @IQVerify (<http://www.iqverify.org.uk>)
- Whether the security contractor is a member of a trade association. If so, you can contact the relevant trade association to find out what checks it makes on companies/consultants joining them. You can also find out some information about the company you are considering using. Some examples of such trade associations are:
 - British Security Industry Association (<http://www.bsia.co.uk>)
 - Association of Security Consultants (<http://www.securityconsultants.org.uk>) – (The Security Consultancy standard is BS 8549)

If you are contracting out your monitoring then, depending on your monitoring requirements, you will need to consider:

- In the case of a security company providing contract monitoring staff to work in your CCTV monitoring centre, whether they meet the requirements of BS 7958 and are also licenced by the Security Industry Authority (<http://www.sia.homeoffice.gov.uk>).
- For remote security monitoring centre monitoring of your CCTV systems, whether the company meets the monitoring parts of BS7958. However, it is important to note that you, as the owner of the system, would still be responsible for the owner requirements in BS 7958. The split of responsibilities would have to set out in the contract. The SIA licence requirements (<http://www.sia.homeoffice.gov.uk>) are applicable to the remote security monitoring centre. If the remote CCTV Monitoring centre also carries out other security monitoring requirements (Intruder alarms, etc.) then it should meet the requirements of either BS 5979 or BS 8591
- Whether your potential security contractor has full knowledge of the SCCoP and the ICO CCTV CoP and how your CCTV system should meet the principles contained within them
- If your potential security contractor is using sub-contractors, whether the contract states the requirements you expect from any sub-contractors used

3.2.4 Making decisions and contracting

Once you have made your decision, when preparing the contract there are some issues that should be taken into account. Remember, you may be using more than one security contractor e.g. one security contractor for CCTV system design, a second security contractor for installation and a third security contractor for maintenance.

- If you are using more than one security contractor then you may need more than one contract
- You should ensure that any software licences are registered in your name rather than the security contractor. Otherwise the security contractor has the licence for your system and only they can update it
- All passwords and the network design should be in your name so that you can change security contractors if you wish
- Ensure that the image export facility meets the statement of need i.e. It can meet the forensic integrity of the recorded image for the purpose for what the CCTV system was intended (See SCCoP Principle 1 and 11)
- You should ascertain responsibilities under Health & Safety legislation and if appropriate the Construction (Design and Management) Regulations (CDM 2015) and ensure that these are properly reflected in the contract

The tender process and contract agreements will invariably depend on local systems and budget sign off authorities. It is strongly recommended that you should contact your contracts department and/or legal departments for more information and advice in preparing the contract. They may also be responsible for preparation of the actual tender and contract documents.

3.3 Installation

3.3.1 System installation

You should make sure that the security contractor is fully aware of the SCC recommended standards for the CCTV industry (<https://www.gov.uk/recommended-standards-for-the-cctv-industry>).

The main standards the security contractor will use are:

- BS EN 62676 - 1-1 – Video surveillance systems for use in security applications. System requirements – General requirements
- BS EN 62676 - 2-1 – Video surveillance systems for use in security applications. System requirements. Performance requirements for video transmission
- BS EN 62676 - 2-1 – Video surveillance systems for use in security applications. Video transmission protocols – General requirements
- BS EN 62676 - 2-2 – Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on HTTP and REST services
- BS EN 62676 - 2-3 – Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on Web services
- BS EN 62676 - 3 – Video surveillance systems for use in security applications. Analog and digital video interfaces
- BS IEC 62676 - 4 – Video surveillance systems for use in security applications. Application guidelines
- BS 8418 – Installation and remote monitoring of detector-activated CCTV systems. Code of practice
- BS 7671 – Requirements for Electrical Installations. IET Wiring Regulations

Control Room requirements are set down in BS 7958. For remote monitored CCTV control rooms BS 7958 or 7499 can be used. If the control room is used for other monitoring purposes then it should meet BS 5979 or BS5891.

3.3.2 System commissioning

BS62676 section 15 outlines the required standards for system installation and commissioning.

A documented system test procedure should be developed, based on the design specification, and this should be used to verify all the functions and the performance of the CCTV system. Any deviations from the expected performance should be noted. In particular, tests should be carried out to verify:

- Camera's field of view
- Image detail
- Live and recorded image quality
- Storage time provided by the system
- Operation of the alarms and motion detection features

Some sample images should be recorded and exported from each camera. This can be used as a reference of image quality and camera field of view during future system maintenance operations and will highlight any change or image degradation that may occur in the system over time.

3.3.3 User acceptance test

It is recommended that there should be an acceptance test plan and that it follows the requirements set out in BS IEC 62676 – 4 Section 13. Part of this test plan will be to ensure that the field of view and image quality from each camera allow you to see the target with the required level of detail (i.e. enables

you to either read a number plate or otherwise monitor the target as set out in BS IEC 62676-4 Section 13 using Annex B, Annex C & Annex E).

A set of test targets (as described in 62676-4) is available from the Home Office Centre for Applied Science and Technology and it is recommended that these are used as a simple means to check image quality. For more information on test target manufacture or to purchase kits you can email CAST at castenquiries@homeoffice.gsi.gov.uk.

The live or on-screen view should be checked for the following:

- Does the picture provide a suitable frame rate for the activity being monitored?
- Is the picture of sufficient quality for the operator to effectively perform their monitoring tasks?
- Do the images meet the specification at the required time of image capture and monitoring (i.e. day and night (is illumination sufficient?))?

Once the live camera view has been checked, it is vital that the quality of the recorded images is also assessed to confirm that there has not been an unacceptable loss in detail during the recording process. The recorded picture should be checked for the following factors:

- Does the picture provide a suitable frame rate for the activities to be reviewed effectively?
- Is the picture of sufficient quality for the reviewer to effectively perform their tasks?
- Is the imagery viewable by anyone who needs to have access to it in order to perform their role?
- Can the content be extracted from the system simply, in sufficient volume and in a suitable format?

At the acceptance test stage, you should also:

- check all the functions (including Pan Tilt Zoom pre-sets and control joy stick controls)
- register any discrepancies and actions to resolve
- check that all documentation (user manuals, system site plans, equipment lists, etc.) is complete and correct
- check that the appropriate operator training been given

See BS IEC 62676-4 Section 15.3, which provides more information and guidance in relation to this.

3.3.4 CCTV system handover

The checklist below lists those issues that you need to consider during the handover process.

- | | | |
|---|------------------------------|-----------------------------|
| Has all of the system documentation been provided?
(See BS IEC 62676 -4 Section 16) | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Have you been provided with a declaration of conformance to standards?
See BS IEC 62676 – 4 Section 15.4. | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Have details of any user maintenance required and details of any consumables required to carry out this task been agreed and provided? The contractor(s) may provide an initial stock of consumables at this stage. | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Have details of any ongoing maintenance requirements been agreed and provided? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Have you confirmed any reference images agreed at the user acceptance test? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Have you been provided you with any equipment warranties, if appropriate? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Have you been provided with all the passwords for the system? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Have you been provided with details of any ongoing training requirements? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

3.4 Maintenance

There are three types of maintenance on a CCTV system these are:

- User maintenance – This maintenance is the day-to-day maintenance carried out by the user to ensure the system meets its performance. This maintenance will be detailed in the handover documentation
- Corrective maintenance is when a fault occurs on the CCTV and your security contractor should provide an engineer to attend site (or remotely by a web interface) to correct the fault (See BS IEC 62676-4 Section 17.1 Section 17.3)
- Preventive maintenance is a maintenance service to maintain the CCTV system to the equipment manufacturers’ requirements and to ensure that the CCTV still meets the agreed specification (See BS IEC 62676-4 Section 17.1 and Section 17.4)

Further information and guidance about system maintenance please refer to the maintenance section of the Technical Specification guidance (Stage 1, section 2).

3.5 Monitoring and audit

3.5.1 Monitoring CCTV system use

Once the CCTV system is installed and the hand over complete a number of factors need to be considered when monitoring your CCTV system use and these are outlined in the checklist below. In addition to checking that you conform to each of the requirements, you should also be able to provide evidence in that regard. For example, you need to be able to provide evidence that the images are only stored for as long as necessary.

You might want to adopt a Red, Amber, Green (RAG) assessment process for your level of conformance i.e. Green for full conforming, Amber for partially conforming and Red for not conforming. You may however have your own method of recording conformance.

FACTOR	CONFORM	EVIDENCE
Does the management and operation of the CCTV system meet the requirements of BS 7958? (See SCCoP Principle 8).		
Is ongoing training of personnel provided if equipment is updated or procedures are changed?		
Is vetting of new personnel, with access to the images, provided?		
Are Privacy Impact Assessments carried out if cameras are added or changed? Please see PIA template in section 1.6 of the Stage 1, Section 1 guidance for further details		
Is maintenance carried out according to BS IEC 62676-4 Section 17? (See SCCoP Principle 8).		
Are there clear rules on responsibilities for the CCTV system activities? (See SCCoP Principles 4 and 5).		
Is access to the images restricted and are there clearly defined rules on who can access the images? (See SCCoP Principles 7 and 9).		
Are the images only stored as long as necessary? (See SCCoP Principle 6).		

FACTOR	CONFORM	EVIDENCE
Are the operators aware of the effect that a CCTV system has on the public and when appropriate, publish contact details for access and complaints about the system? (See SCCoP Principles 2 and 3).		
Does the export of images from the CCTV system meet the police/courts requirements? (See SCCoP Principle 11).		
If the CCTV system images are being used to match against another data base, is that database being kept up to date? (See SCCoP Principle 12).		

You should consider developing a schedule or plan to ensure that such monitoring takes place on an ongoing basis. The guidance in section 3.1 above may be able to help in this regard.

3.5.2 Audit

The cameras fields of view should be checked periodically as required by the maintenance contract to ensure that the views are as specified in the original operational requirement. Camera housings might have moved, fixings may corrode or other elements may be added to the scene to obscure the view.

A useful auditing tool is to undertake a periodic system walk round. This activity should include every camera in the system, and at each camera you should identify the useful field of view, point of focus, depth of field and efficiency of any alarms. It is worthwhile carrying this out when the preventive maintenance cycle is due so that the engineer can aid you and that any difference in image quality for the initial images or viewing areas can be dealt with at the time.

Other factors that should be considered when carrying out an audit of your CCTV system are outlined in the checklist below. Once again, in addition to checking that you conform to each of the requirements, you should also be able to provide evidence in that regard.

FACTOR	CONFORM	EVIDENCE
Is the justification for the system (Decision Point 1) still valid? A review of factors considered up to Decision Point 1 will be required if there have been any changes to the system.		
Are the objectives (section 1.2) and statement of need (section 1.4) being met? If they are not being met over the longer-term, you may have to explore why this is. It may require modifications to the system. If the system fails to meet the statement of need over the longer-term (SCCoP Principle 1, ICO CCTV CoP) then the system should be shut down (SCCoP Principle 2 and Principle 11)		
Is the Privacy Impact Assessment (PIA) still valid? Please see PIA template in section 1.6 of the Stage 1, Section 1 guidance for further details		
Are all the principles in the SCCoP and the ICO CCTV CoP being met?		
Have you completed the online Surveillance Camera Code of Practice self-assessment tool to ascertain if your organisation's CCTV system complies with the 12 principles contained within the codes? If not, you are encouraged to do so.		

FACTOR	CONFORM	EVIDENCE
Has your CCTV system achieved third party certification to the principles contained within the Surveillance Camera Code of Practice?		
Are all applicable legal requirements being met? (e.g. RIPA).		
Are all of those involved in the collection and distribution of CCTV images correctly trained? If not, you should carry out a training review and use the findings to develop and implement an appropriate training program.		
Do all of those who have access to the CCTV images meet the relevant security requirements (vetting).		
Have you reviewed all contracts with suppliers to ensure that they remain relevant and appropriate?		
Have you produced an annual report outlining the progress made during the year and the results of systems monitoring and audit?		

You should again consider developing a schedule or plan to ensure that such an audit takes place at the appropriate times and delivers within the required timescales. The guidance in section 3.1 above may be able to help in this regard.