


CPNI Control Rooms Guidance

Helping you get the most out of your control room

 [Read disclaimer](#)

© Crown copyright 2016. This guidance is available under the Open Government Licence v3.0.

Disclaimer: This guidance is issued by the UK's Centre for the Protection of National Security (CPNI) with the aim of helping organisations that make up the national infrastructure improve their protective security. It is general guidance only and needs to be adapted for use in specific situations. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any expense, liability, loss or proceedings incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. You should make your own judgement as regards use of the guidance and seek independent advice as appropriate.

1. UNDERSTANDING AND PLANNING

2. DESIGN AND BUILD

3. BUSINESS AS USUAL

4. INCIDENT RESPONSE

5. EXERCISES

Operational requirement: overview



A **Level 1 Operational Requirement (OR)** is used for protecting critical assets against security threats. When you carry out a Level 1 OR, you:

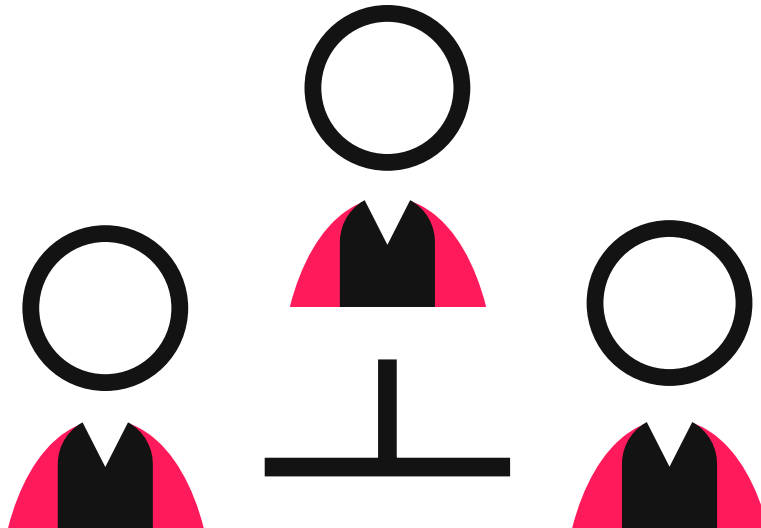
- assess security risks
- identify risk mitigation options
- evolve and justify the actions that need to be taken and investments to be made.

A **Level 2 OR** addresses individual security measures. It should be carried out when there are any:

- alterations
- design changes
- new control rooms.

-
- [!\[\]\(0f48f43ebd21f231a458c96216dbf4d1_img.jpg\) Read more about Operational requirement](#)
 - [!\[\]\(ba0878532603d6e0b20c60ffb7475d12_img.jpg\) You may also want to read about Culture: overview](#)
 - [!\[\]\(0a70dbd9915c9ea99c6f238a2c711f53_img.jpg\) You may also want to read about Use case: overview](#)
 - [!\[\]\(76511d025e9c8b0592325ddba91331d4_img.jpg\) You may also want to read about Threat: overview](#)
 - [!\[\]\(4ecf357067dff2cd4f65e9b71acfab07_img.jpg\) You may also want to read about Hostile reconnaissance: overview](#)
 - [!\[\]\(bdcc6b43570ac03740a9b9fceebadffe_img.jpg\) Go to 1. Understanding and Planning](#)
 - [!\[\]\(19e7888cfa74401aed481c3fe14d7758_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(f030a72b34d8705fb3a85bf642ca0dcf_img.jpg\) Go to Glossary](#)

Culture: overview



When planning a control room you should consider the security culture of your organisation as it has an effect on how the control room functions.









It is useful to clarify the role of the security department within the organisation to prevent any misunderstandings from the rest of the organisation.

SECURITY IS

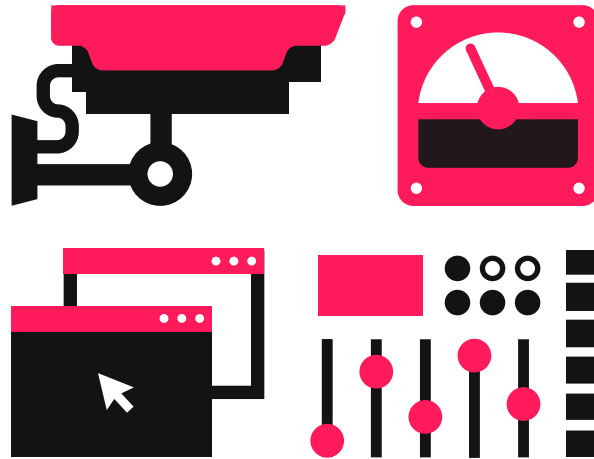
- everyone's responsibility, not just the security department's
- there to keep you safe
- there to enable operations.

SECURITY IS NOT there to

- provide dialling codes
- receive parcels
- take in lost property.

-
-  Read more about [Culture](#)
 -  You may also want to read about [Operational requirement: overview](#)
 -  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Hostile reconnaissance: overview](#)
 -  Go to 1. [Understanding and Planning](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)

Use case: overview



The modern control room is usually more than a CCTV monitoring station. It may:

- use PIDS (Perimeter Intruder Detection Systems) to maximise security and response
- monitor events live or after the event
- link with other control rooms.

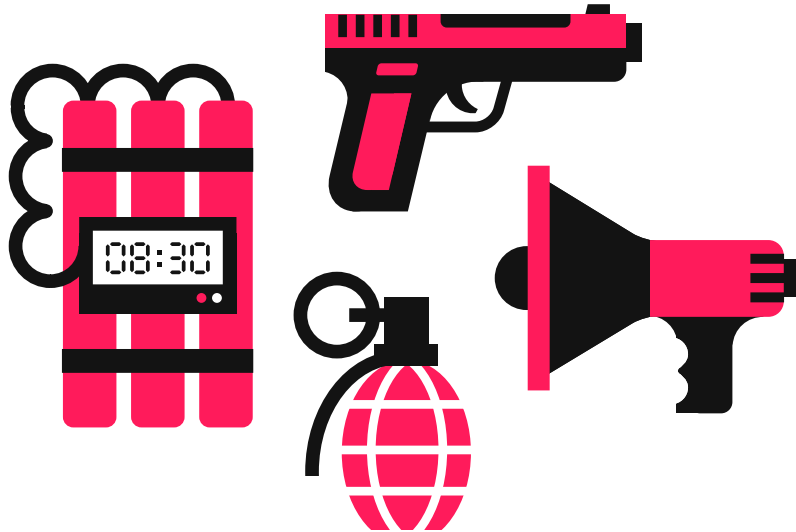
You may also consider whether you want to use CCTV footage as evidence, such as images for identification.

Depending on the size of your site and your guard force, you may also want to:

- determine defensive lines
- decide on points at which an attacker should be detained to stop them reaching any critical asset.

-
- [!\[\]\(e27c4336460e9e6729a19580c0456728_img.jpg\) Read more about Use case](#)
 - [!\[\]\(1a140e8db538fd46d58af9f9540232fd_img.jpg\) You may also want to read about Operational requirement: overview](#)
 - [!\[\]\(5a658b86f2c8900a276c586c1f8f9f2f_img.jpg\) You may also want to read about Culture: overview](#)
 - [!\[\]\(dde796100cc481a63a6f917e6942c754_img.jpg\) You may also want to read about Threat: overview](#)
 - [!\[\]\(63a8f188d537bd691c8d94f41db6869a_img.jpg\) You may also want to read about Hostile reconnaissance: overview](#)
 - [!\[\]\(499fe69158060e68a02a9089268949e0_img.jpg\) Go to 1. Understanding and Planning](#)
 - [!\[\]\(c8aba30b21c2fae4d961d3c29bf22065_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(b5c199051809cfc34ae5dec3ec9d2866_img.jpg\) Go to Glossary](#)

Threat: overview



Your site might be a target for many types of hostile intentions, such as:

- extremism
- espionage
- protests
- organised crime.

Each type of threat will need to be considered separately – what is useful to counter one threat may not work against another threat.

You should tailor the measures for your site to the threat profile for that site, and consider highly likely and high consequence threats.

-
- [!\[\]\(e492b5d52ab457a7a3c2826c4091dfee_img.jpg\) Read more about Threat](#)
 - [!\[\]\(1d9440fab1f214291ce1c26a75f9c2cd_img.jpg\) You may also want to read about Operational requirement: overview](#)
 - [!\[\]\(6be2e1cb461308cfbb51376f893366b1_img.jpg\) You may also want to read about Culture: overview](#)
 - [!\[\]\(9d1c9e561b4c39f4d970a841cbc526df_img.jpg\) You may also want to read about Use case: overview](#)
 - [!\[\]\(638c4e65afbf8f3994df6311f702c5cb_img.jpg\) You may also want to read about Hostile reconnaissance: overview](#)
 - [!\[\]\(ac8167fe1d77dc734374ed4531294f8f_img.jpg\) Go to 1. Understanding and Planning](#)
 - [!\[\]\(fff2f1ab464b6499fbd670c53975d01d_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(81d285ad7149d05e4bfce88826a8e29e_img.jpg\) Go to Glossary](#)

Hostile reconnaissance: overview



Hostile reconnaissance is the gathering of information that can be used to plan further action.

Information gathered is used to:

- identity weaknesses
- assess the likelihood of success
- plan an attack.

This gives security managers an absolutely crucial opportunity to block any action by:

- disrupting the hostile reconnaissance
- getting the message across that your site is a tough target and an attack is unlikely to succeed.

-
- [!\[\]\(e6ddc77b791299d975007937cebef274_img.jpg\) Read more about Hostile reconnaissance](#)
 - [!\[\]\(ab52e27d061d76db54e182891376cff5_img.jpg\) You may also want to read about Operational requirement: overview](#)
 - [!\[\]\(62325268b83c539c826661482098edc3_img.jpg\) You may also want to read about Culture: overview](#)
 - [!\[\]\(576eae82d6cd110cfd50d3e0356faa5a_img.jpg\) You may also want to read about Use case: overview](#)
 - [!\[\]\(433d19d9bdeac46075af10d8acb0c69a_img.jpg\) You may also want to read about Threat: overview](#)
 - [!\[\]\(6d7be85c6a97460dda8fae4160076286_img.jpg\) Go to 1. Understanding and Planning](#)
 - [!\[\]\(6821accee9ffc315d041eee2faac4aff_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(a429abaf87b67f8fc452687d739f1fb1_img.jpg\) Go to Glossary](#)



Operational requirement

WHY CARRY OUT A SYSTEMATIC OPERATIONAL REQUIREMENT (OR)?

- To record user and operational needs.
- To recommend appropriate security measures that manage risks to an acceptable level.
- To structure the way you determine security.

THERE ARE TWO LEVELS OF OPERATIONAL REQUIREMENT – LEVEL 1 AND LEVEL 2

Taken together, they will provide a full picture of the integrated security solution. This will include security and non-security considerations.

Level 1 Operational Requirement

A Level 1 OR is the main statement of the overall security need.

It should involve all stakeholders – security managers, building owners, the people who work in and use the building, those responsible for maintenance and support requirements, and operators of the current and proposed technical security systems.

In a Level 1 OR, you define:

- The site or building that the OR covers
- Assets to be protected
- Perceived threats (and probability of their occurrence) against the assets or adjacent facilities
- Consequences if assets are compromised or damaged
- Physical areas that contain the assets to be protected, and perceived
- Vulnerabilities of those areas to the threat(s)
- What success looks like.

Level 2 Operational Requirement

A Level 2 OR covers individual security measures such as fences, CCTV or control of access in more detail.

The Level 2 OR will be the basis for your systems requirements document, or technical specification that can be used for tendering and during test and evaluation.

Whenever there's any alteration or design change in a control room, or you are building a new control room, you'll need to carry out a Level 2 OR.

The Level 2 OR enables you to create checklists that inform the detail that the designer needs, for performance specifications covering possible solutions.

These performance specifications will spell out parameters for proposed systems, and help people involved make informed decisions when procuring security risk management on the site.

It's important to integrate your new Level 2 OR with other relevant Level 2 ORs, and ensure that all technologies in the control room are compatible and work together.

WHEN SHOULD YOU CARRY OUT THE CONTROL ROOM OR?

Ideally you should consider the control room Level 2 OR while the site is being planned, before construction begins.

During the initial OR process – the design overview








If the control room is considered as early as possible in the design and construction phase, you can achieve a control room that is fit for purpose, and maximise security and value for money.

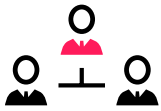
If you only start thinking about the control room late in the design and construction process, you may find that you end up squeezing it into the last remaining bit of space (and a less than ideal location). This in turn may mean the control room is unproductive and poor value for money.

Mapping the details during the site design process

If you START by carrying out a control room Level 2 OR, (before other security Level 2 ORs) you may limit the capacity of the overall security solution to the specifications of the control room. (You could end up with a control room just big enough for two security officers, or limit your site security to 100 CCTV cameras with no other functions.)

If you wait to do a control room Level 2 OR until AFTER other ORs are completed, you'll have a better overview. You'll be able to specify the control room to maximise the overall security solution and provide best value for money.

-
-  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Culture: overview](#)
 -  You may also want to read about [Hostile reconnaissance: overview](#)
 -  Go to [1. Understanding and Planning](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Culture

When planning a control room you should **consider the security culture of your organisation** as it has an effect on how the control room functions.

It's useful to **clarify the security department's role within the organisation** to prevent any misunderstandings. This can help your security team's motivation and performance, and increase the understanding and status of security in the wider organisation.

START BY MAKING IT CLEAR TO EVERYONE WHAT SECURITY IS AND WHAT IT DOES NOT DO



Security is

- everyone's responsibility, not just the security department's
- there to keep you safe
- there to enable operations.



Security does not

- provide dialling codes
- receive parcels
- take in lost property.

As well as the physical, technical and information aspects of security, the people within an organisation shape its security culture by the way they act and how they think about it.

Where the culture is strong, employees will tend to be more aware of security in how they think and act.

They'll be likely to:

- remember the values of the organisation that they work for
- behave in ways that protect its reputation
- be aware of what might threaten business impact and ultimately national security.

This behaviour might include following a clear desk policy, and managing their digital footprint.

When managers and staff at all levels understand and respect the organisation's security culture, it will be more effective and strengthen the planning and implementation of security values, behaviours and actions. That will lead to:








- **greater employee engagement**
- **reduced risk and vulnerability** where employees are encouraged to think and act in more security conscious ways
- **reduced risk of reputational or financial damage** as staff are security conscious
- **improved organisational performance** where people are trained and understand the security aspects of their role.

If your security culture is effective, your organisation may see wider benefits such as improved team working, increased employee satisfaction, and higher levels of commitment to the organisation. And that can all add up to a healthier bottom line.

And there's another important asset that stems from strong security culture and associated work behaviours: the deterrent effect. Where visitors and VIPs see staff who are clearly alert and vigilant, this can deter people with hostile intentions.

FURTHER READING

- **SeCuRE 3, CPNI's security culture survey tool**
- **My Digital Footprint asset library**

-
-  You may also want to read about [Visitors to the control room: overview](#)
 -  You may also want to read about [Staff training](#)
 -  You may also want to read about [Shifts: overview](#)
 -  You may also want to read about [Recruitment: overview](#)
 -  Go to [1. Understanding and Planning](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Use case

What is your control room there to achieve? Does it have a primary use?

Many modern control rooms are not simply CCTV monitoring stations – they are linked with other security solutions to maximise security and response, such as:

- **Intruder Detection Systems (IDS)** to maximise security and response
- **Monitoring events as they happen** – well-motivated and proactive security guards will be required to detect and respond quickly to situations
- **Links with other control rooms** such as an operational control room to maximise the information flow
- **Post-event monitoring** where you may want to analyse what happened

Depending on the size of your site and your guard force, you may also want to determine:

- defensive lines
- points where any attacker should be detained to stop them reaching a critical asset.

SUCCESS CRITERIA

A realistic approach is essential, so you'll need to agree the critical ('must have') and aspirational ('nice to have') points of defence and intervention. Depending on your site, it may not be practical to consider the perimeter as the line of defence.

FOR EACH SCENARIO, WORK THROUGH THE LOGICAL SEQUENCE

Event >	Location >	Event type >	Action
Protestors	At the outside perimeter	Information	Monitor what's going on
A potential intruder	At the fence line	Potential	Send a security officer to check it
Someone has breached the fence	At the fence line	Perimeter breach	Send a security officer to check it
Someone has breached an administrative building	Non-vital building	Non-vital breach	Phone staff for confirmation
Someone has breached a secure building	Vital building	Vital breach	Phone emergency services

It's also important to work out what success looks like – again, this will depend on the size of your site and its type. You may be monitoring a single building, a railway station, a shopping centre or a power plant: your success criteria will depend on what you want to achieve or what you must prevent.

For example, if someone with hostile intent may be heading for a critical area, your control room will need to be able to detect and track them.

FACTOR IN DETECTION TIME WHEN CALCULATING TARGET RESPONSE TIMES

Inevitably the total delay until an event is resolved (for example, when security officers can report on an event or intercept a potentially hostile intruder) will be longer than detection time + officers' response time.

You'll also need to take account of any obstacles (fence, wall, access control systems) that could delay the officers on their way to the event. In the same way, response time may be longer if security officers have to search the entire site rather than focus on a 50-metre section of fence.

Detection time may depend on how frequently a security officer checks that specific point – for example, a guard checks the front gate at 10:00 and then at 10:10, there could be a delay of up to 10 minutes before an event is detected and the response is set in motion.









Where an IDS (Intruder Detection System) is in operation, the number of guards required to secure the site may be reduced.

TEST YOUR PLAN

Whatever your plan to protect your site, it's a good idea to carry out simulations and exercises from time to time, to check:

- response time
- delay time
- whether the response is efficient and appropriate.

At the end of the exercise, the people involved should be debriefed and any lessons learnt should be collated and incorporated into the overall plan.

-
-  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Types of guard force and control room: overview](#)
 -  You may also want to read about [Security officers: overview](#)
 -  You may also want to read about [Control room: overview](#)
 -  You may also want to read about [Exercises and simulations: overview](#)
 -  Go to [1. Understanding and Planning](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



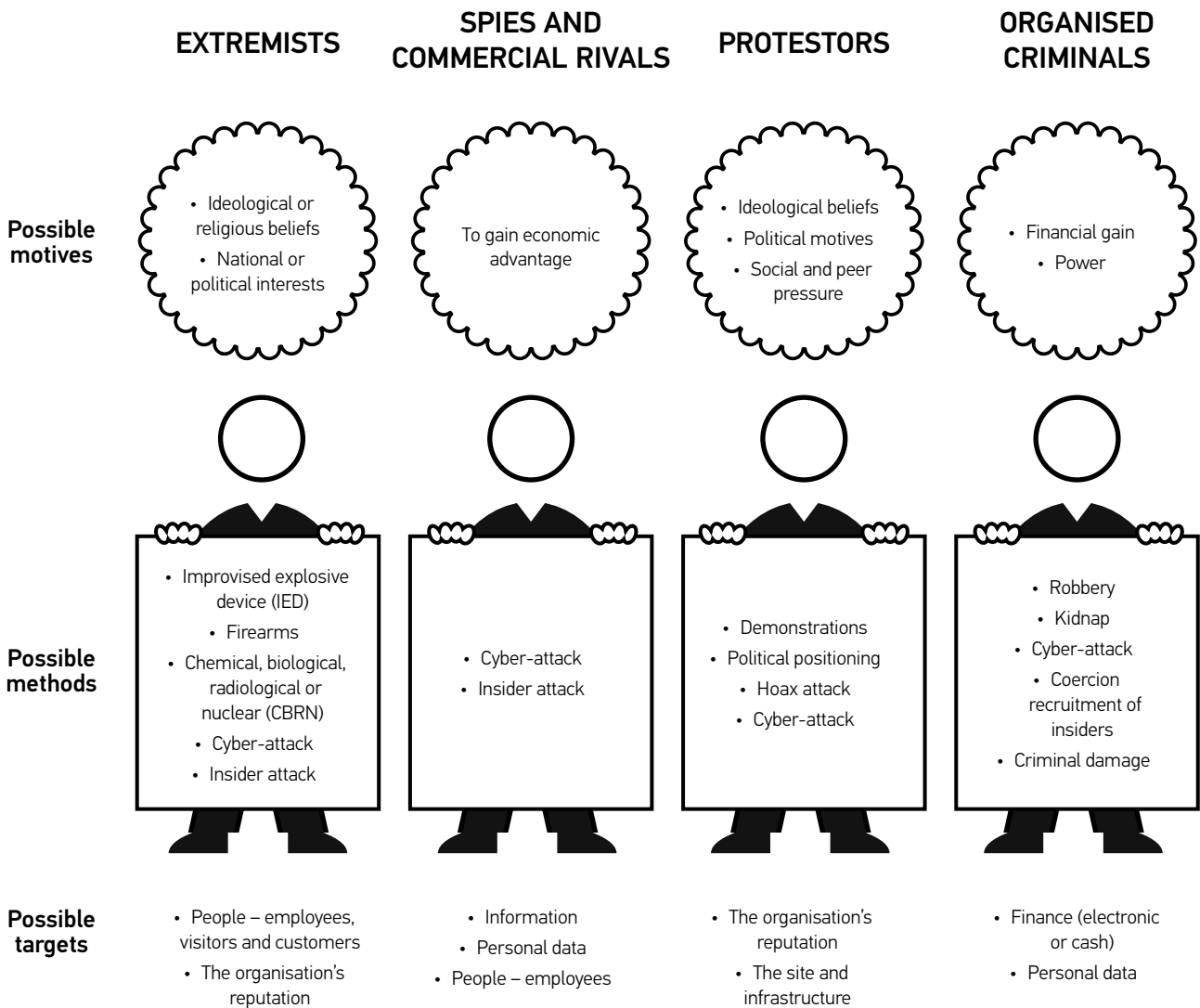
Threat

If yours is a CNI (Critical National Infrastructure) site, it could be the target for many types of hostile intentions.








These could include:

- **extremism** – maybe because the site has a lot of people
- **espionage** (cyber-espionage or ‘old-fashioned’ physical spying) – maybe because your organisation/site is of considerable commercial interest
- **protests** – for example when the organisation has been the focus of negative media coverage
- **organised crime** – particularly where significant financial and personal data is held in the institution’s data centre, or a lot of cash is kept on site.

This is not an exhaustive list, but below you’ll see an idea of topics to cover when you are considering possible threats to your site.



It's best to consider each threat (and ways to mitigate it) separately, and to tailor the threat profile to your site by considering which threats are more likely and would have the most serious consequences.

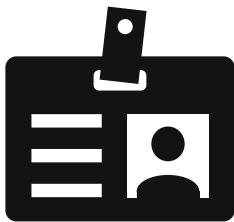
-
-  You may also want to read about [Hostile reconnaissance: overview](#)
 -  You may also want to read about [Types of guard force and control room: overview](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Response: overview](#)
 -  Go to [1. Understanding and Planning](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



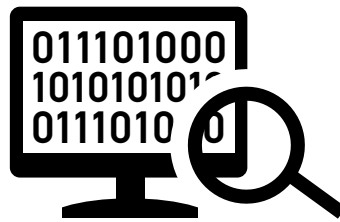
Hostile reconnaissance

Hostile reconnaissance is the gathering of information that can be used to plan further action against a site or an organisation.

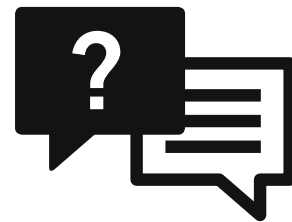
WAYS THAT PEOPLE WITH HOSTILE INTENT MAY GATHER INFORMATION



On-site visits



Online research



Insider knowledge

The information gathered is used to:

- identify weaknesses in security
- assess how likely they are to be detected during the reconnaissance and any action
- plan an attack.

Security managers have a crucial opportunity to block any action by disrupting the hostile reconnaissance and getting the message across that your site is a tough target.

As well as understanding the assets that your control room is there to protect, it's worth considering what might motivate people with hostile intent to attack your site:

- **intent** – their overall aim and the effect they want to achieve
- **capability** – the resources they have access to (equipment, time, personnel, skills, finance and location)
- **culture** – their personal motivation and their appetite for risk.



DENY



DETECT




DETER

These three words sum up the main ways to disrupt hostile reconnaissance.

If your team can detect hostile reconnaissance, it may help you in situations where the attacker might reach key assets faster than a response team could get there.


	Online	On site
Deny	<ul style="list-style-type: none"> Remove useful information about site and people who work there Create uncertainty about security measures Prevent external access to IT systems 	<ul style="list-style-type: none"> Unpredictable security Staff not susceptible to social engineering Robust entry processes
Detect	<ul style="list-style-type: none"> Cookies tracking Use of virtual assistants/ avatars (“Hi I see you’re looking at our security page, can I help?”) Encourage staff to report spear phishing (emails that seem to be from known contacts, designed to access passwords or financial information) or other attempts by hackers to trick people into security breaches. 	<ul style="list-style-type: none"> Vary security routines – don’t be predictable Encourage everyone (staff and members of the public) to report anything suspicious Vigilant security officers are effective Proactive CCTV Deploy maximum detection measures in key areas ‘Join the dots’ – integrate your security measures
Deter	<ul style="list-style-type: none"> Publicise DENY and DETECT – let it be known that you use a range of integrated detection capabilities from staff vigilance to CCTV 	<ul style="list-style-type: none"> Posters and other on-site communication tools such as public audio announcements publicising DENY and DETECT Staff/public vigilance posters Be seen to be vigilant If anyone is watching, they’ll see CCTV cameras moving, security officers who are vigilant and integrated security measures in key areas.

 You may also want to read about [Threat: overview](#)

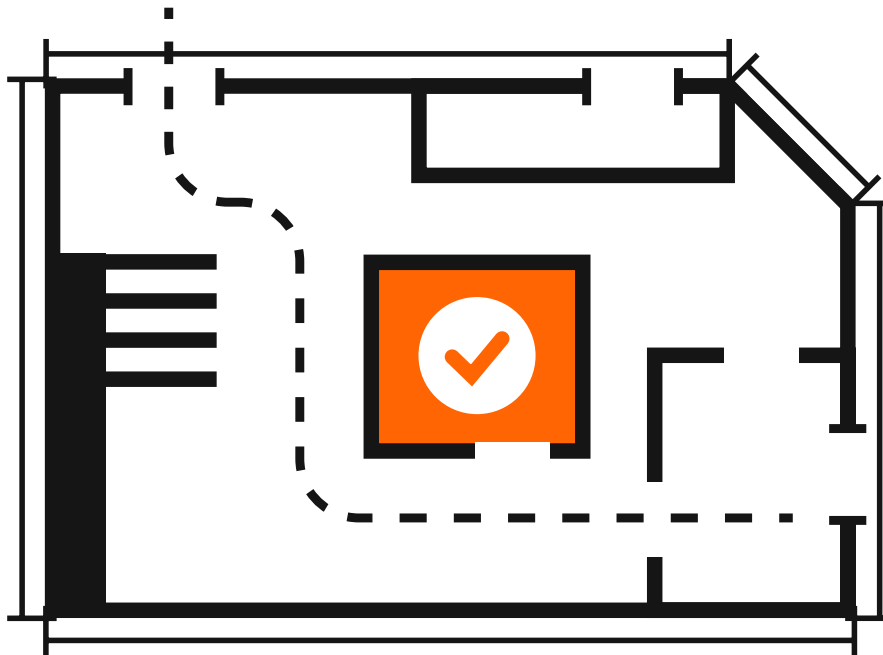
 You may also want to read about [Monitoring CCTV](#)

 Go to [1. Understanding and Planning](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)

Control rooms: overview



Ideally your control room should be located away from the site perimeter.

Where you choose to place it will depend on:

- the use of the control room – whether it needs to be co-located with operations or another function
- the threats to the site.

It's a good idea to consider where to locate your backup control room, too.

Your people are your prime asset: when you plan the physical design of your control room, it's important to consider their needs and comfort as well.

-
- i** You may also want to read about [Location of your control room](#)
 - i** You may also want to read about [Incident rooms](#)
 - i** You may also want to read about [Security officers: overview](#)
 - i** You may also want to read about [Room layout](#)
 - i** You may also want to read about [How secure does your control room need to be?](#)
 - ↗** Go to [2. Design and build](#)
 - ↗** Go to start of [Control Rooms Guidance](#)
 - ↗** Go to [Glossary](#)

Types of guard force and control room: overview



How your control room works will be largely determined by the people within the control room and the type of guard force you use.

- An **employed guard force** may cost more, but have higher vetting levels, understand your business and potentially make more relevant decisions.
- A **contract guard force** may be cheaper and able to cover sick leave, but may only have basic training and have inappropriate Key Performance Indicators.

Where your security officers are based is also a factor:

- Security officers in an **on-site SCR** (Security Control Room) may have better situational awareness and quicker response times.
- A guard force in an **offsite SCR** will have reduced situational awareness and an extended response time.
- An **ARC (Alarm Receiving Centre)** will only monitor and respond to what it is paid to monitor, and will be covering a number of sites and businesses.

-
- i** You may also want to read about [Location of your control room](#)
 - i** You may also want to read about [Security officers: overview](#)
 - i** You may also want to read about [Room layout](#)
 - i** You may also want to read about [How secure does your control room need to be?](#)
 - ↗** Go to [2. Design and build](#)
 - ↗** Go to start of [Control Rooms Guidance](#)
 - ↗** Go to [Glossary](#)

Security officers: overview



How many security guards do you need?

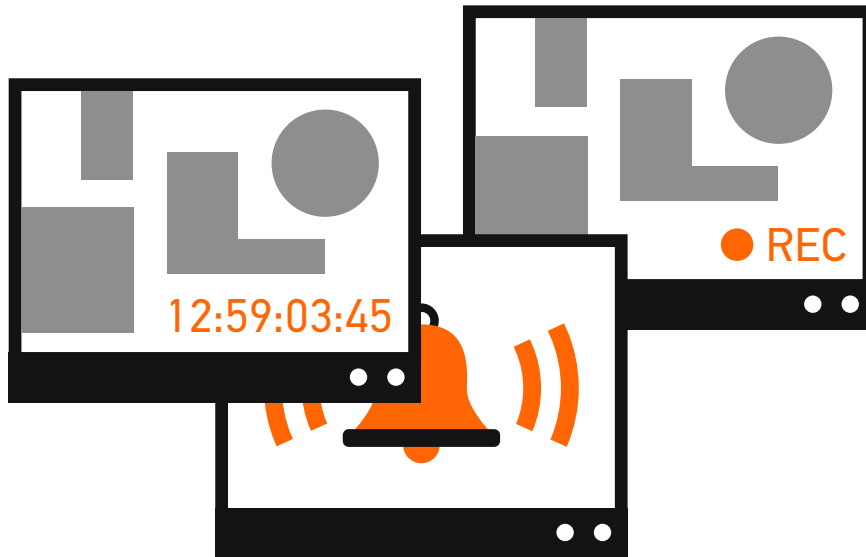
It depends on what they have to do – that might include any or all of these tasks:

- monitoring CCTV – the busier the scene, the more people you need to monitor CCTV.
- guarding on site
- carrying out patrols
- managing keys and passes.

While they are doing these tasks they will be identifying potential intrusions, keeping an eye on vulnerable areas, and dealing with suspicious people, objects and events. They are also there to help manage incidents.

-
- [i](#) Read more about [Security officers](#)
 - [i](#) You may also want to read about [Roles and responsibilities](#)
 - [i](#) You may also want to read about [Training: overview](#)
 - [i](#) You may also want to read about [Shifts: overview](#)
 - [i](#) You may also want to read about [Monitoring CCTV](#)
 - [i](#) You may also want to read about [Recruitment: overview](#)
 - [🔗](#) Go to [2. Design and build](#)
 - [🔗](#) Go to start of [Control Rooms Guidance](#)
 - [🔗](#) Go to [Glossary](#)

CCTV screens: overview



It's important not to overload the people who are monitoring the screens – remember that desk displays should be used for primary duties.

Site CCTV screens should show targets at a minimum of 10% for detection tasks. That's the limit of human vision to distinguish between a person, a car or an animal.

In most cases, **three screens on a desk are the recommended maximum:**

- one for CCTV monitoring
- one for alarms from detectors
- one for reviewing recorded CCTV.

If you have a video wall, take care that it doesn't distract people monitoring the CCTV at their desks. It's best used by supervisors for overview and to inform incident management.

i You may also want to read about [Monitoring CCTV](#)

i You may also want to read about [CCTV operation](#)

i You may also want to read about [Screen display](#)

i You may also want to read about [Visual inputs](#)

[↗](#) Go to [2. Design and build](#)

[↗](#) Go to start of [Control Rooms Guidance](#)

[↗](#) Go to [Glossary](#)

Resilience: overview



Loss of the SCR (Security Control Room) can cause major disruption. Recovery from that loss can be expensive both in money and people's time.

Don't rely on technology alone. Make sure you have basic equipment (whiteboards and paper log books etc) as backup so you can collate information when screens aren't working or systems are down.

It's important to train security guards how to work with your backup system (just as they need to learn how to use the everyday equipment).

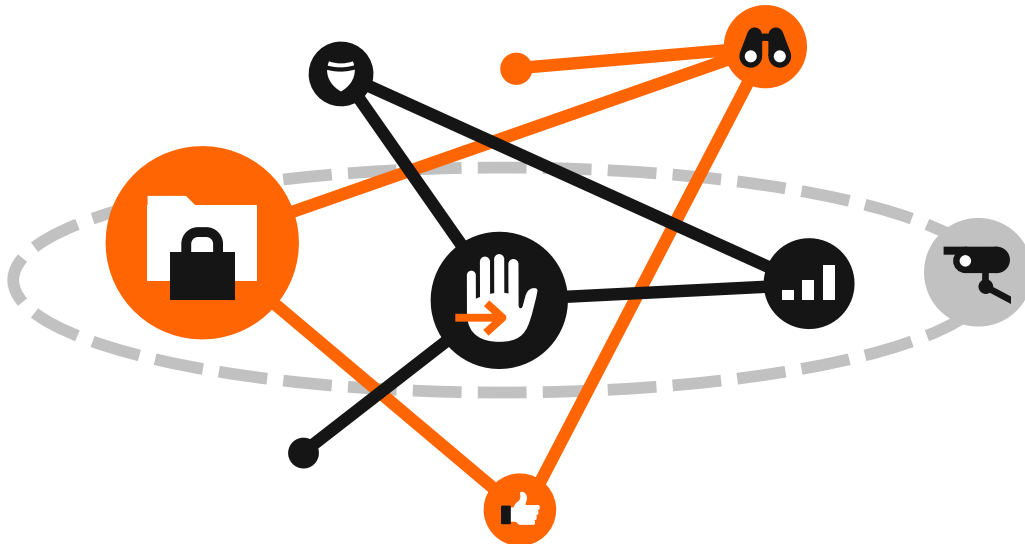
Your control room should be resilient enough to cope with:

- power outages
- extreme weather conditions
- loss of heating or air conditioning.

It's also worth considering setting up a backup SCR. This could be used in the event of a failure of the main SCR. It's essential to train people to work in the backup control room too.

-
- [i](#) Read more about [Resilience](#)
 - [i](#) You may also want to read about [How secure does your control room need to be?](#)
 - [i](#) You may also want to read about [Network security](#)
 - [i](#) You may also want to read about [Network function](#)
 - [i](#) You may also want to read about [Technical integration: overview](#)
 - [↗](#) Go to [2. Design and build](#)
 - [↗](#) Go to start of [Control Rooms Guidance](#)
 - [↗](#) Go to [Glossary](#)

Technical integration: overview



Integration can increase the effectiveness of a control room. It can take the form of **linking technical security measures at different levels:**

- locally at the component level (dual technology IDS detectors)
- locally at the node (such as swipe card controls)
- centrally in the control room (security management system).

It's worth considering how to maintain security, and asking questions such as:

- Is all security on a single point of failure?
- Can the technology fall back to individual systems?
- Are there any unintended effects of integration, and of joining two systems?
- How does integration of non-security systems increase the site's vulnerabilities?

i Read more about [Technical integration](#)

i You may also want to read about [Resilience: overview](#)

i You may also want to read about [How secure does your control room need to be?](#)

i You may also want to read about [Network security](#)

[Go to 2. Design and build](#)

[Go to start of Control Rooms Guidance](#)

[Go to Glossary](#)

User interface: overview



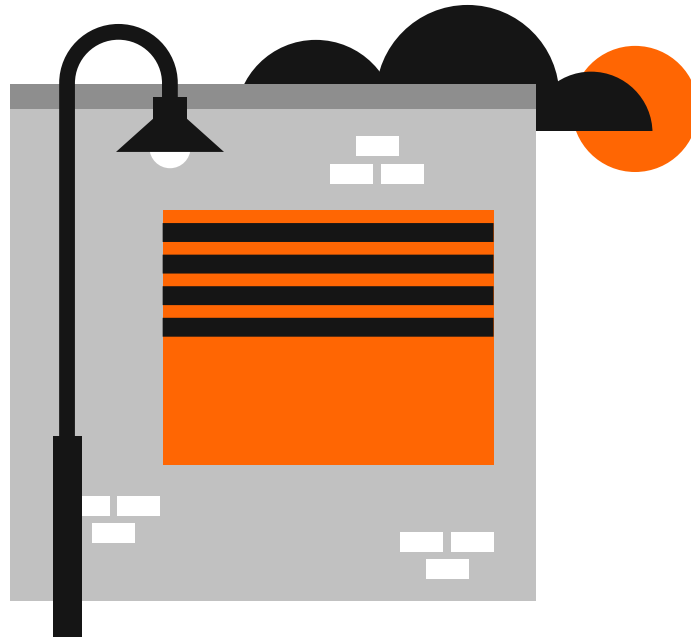
The way information is supplied and shown to the security officer in the control room is critical to maximising the control room's day to day efficiency and its response to an incident.

A well designed user interface can provide:

- greater situational awareness
- better detection
- a faster response to a situation
- a more tailored response to a situation.

-
- [i](#) Read more about [User interface layout](#)
 - [i](#) You may also want to read about [Monitoring CCTV](#)
 - [i](#) You may also want to read about [Technical integration: overview](#)
 - [i](#) You may also want to read about [Screen display](#)
 - [Go to 2. Design and build](#)
 - [Go to start of Control Rooms Guidance](#)
 - [Go to Glossary](#)

Windows and external lighting: overview



When you're designing a control room, you'll need to balance security within the room with the needs and comfort of the people who work there.

In most cases you'll want to ensure that:

- people outside the room can't see in
- at night, the lights inside the room don't make everything inside visible to someone looking in.

You may want to consider whether windows are a good idea – they may make the room more vulnerable, but the people who work in the control room may be happier if they can see out.

-
- [!\[\]\(661ad2fdbe8fa1392f2b194cfa45d124_img.jpg\) Read more about Windows, lighting and temperature](#)
 - [!\[\]\(4193cdf1061c98ac39c3073e7f9019f2_img.jpg\) You may also want to read about Room layout](#)
 - [!\[\]\(4caf182c2ec1a7bf8758f380863453a1_img.jpg\) You may also want to read about Screen display](#)
 - [!\[\]\(1db4d9ef699fa8bfcc76b363f93bcb5b_img.jpg\) You may also want to read about How secure does your control room need to be?](#)
 - [!\[\]\(a2a8d4a709c2c9b96d069b603f10f993_img.jpg\) Go to 2. Design and build](#)
 - [!\[\]\(a9e5ce03a67fbcdb1e4107dd8c6152af_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(06f3659008c9cd9ed3fb5eb301a1c516_img.jpg\) Go to Glossary](#)



Security officers

The number of security officers that you need will depend on what they have to do. This can range from monitoring CCTV, dealing with suspicious items or people and identifying hostile reconnaissance (especially at vulnerable points on the site).

It's important that everyone on the security team – whether they are monitoring CCTV, patrolling the site or managing the control room – has a good knowledge of the site and the perimeter.

When everyone has a clear idea of where the cameras are sited, what the weak points are in the perimeter and where critical assets are located, they'll be better informed and it will help them to communicate with the rest of the team when an incident does occur.

MONITORING CCTV AND ASSESSING VULNERABLE AREAS

The security officers who are monitoring CCTV screens are usually the first to identify an intrusion or an alarm at the boundary.

Typically they may conduct CCTV patrol of an assigned section of the site perimeter, barriers and access control around the secure area.

Bear in mind that if a security officer is covering the maximum number of images, they should not have other tasks to complete at the same time.

If someone really has hostile intentions they will almost certainly prepare for an attack by carrying out hostile reconnaissance beforehand, and they will be looking for the most vulnerable areas.

It's worth thinking about your site's vulnerabilities, for example:

- Look at the fence and gates, and spot any gaps, holes, places where someone might get a hand grip.
- Are there any climbing aids outside the fence, such as street furniture, overhanging trees, vehicles parked beside the fence?
- Identify quiet areas that are not overlooked, where access would be relatively easy. This might vary depending on the time of day and whether the site is working.

DEALING WITH SUSPICIOUS ITEMS OR PEOPLE

Security officers are usually the first people on the scene when there are people acting suspiciously or suspicious items that need to be investigated.

It's important that everyone working in the control room and dealing with incidents on the ground understands:

- how to communicate with their colleagues and managers
- how to gather useful information
- how they intend to block the progress of someone with hostile intentions.









ADMINISTRATIVE DUTIES

Ideally, admin staff will carry out admin tasks such as issuing passes – otherwise this sort of work can distract security officers from their main duties.

If these tasks have to be done by security officers, it's a good idea to rotate the responsibility and use it as a break from monitoring the CCTV display screens. These tasks should be done in a different dedicated area away from the main control room to avoid distracting those officers working on core security tasks.

FURTHER READING

- **CPNI Guard Force Motivation document**
- **CPNI CCTV best practice guide**

-
-  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Shift lengths and task rotation](#)
 -  You may also want to read about [Other control room functions](#)
 -  You may also want to read about [Staff welfare at work](#)
 -  You may also want to read about [Staff recruitment and promotion](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Location of your control room










Where should your control room be located? Does it need to be co-located with operations or any other function? What are the main threats to the site that you protect? External factors such as availability of power or networks may limit your options.

If you locate the primary control room in the centre of the site's secure area, this can provide layers of protection for the control room, maximise security and reduce response time.

It's worth weighing up the pros and cons of locating a control room on the perimeter or near the site's reception area. The control room may be at greater risk from outside threats but it will be safer if an incident occurs at the centre of the site and senior managers might get there faster.

PLAN A SPECIFICALLY DESIGNED BACKUP ROOM AS WELL – DON'T JUST USE ANY OLD LEFTOVER SPACE

It's important that the IT connectivity is secure between the main control room and the backup. If your backup room is unmanned and only used for emergencies, it may be more vulnerable – so make sure it can only be accessed by authorised security officers.

-
-  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Incident rooms](#)
 -  You may also want to read about [Rest areas](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Evacuation and critical staff](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



How secure does your control room need to be?

Is your control room less critical, as critical as or more critical than other aspects of the site? In most cases (unless you have very robust fall-back options) consider giving it the same security level as the most critical asset on the site.

Perhaps you can separate any non-security functions (such as lost property, parcel delivery) from the control room. This can reduce the cost of the control room.

Alternatively you may rate the control room itself as critical and restrict access accordingly, but leave associated support areas such as toilets, kitchen and rest area outside the restricted zone. In this case the security team leaves the high security zone for comfort breaks and rest periods.

The most secure but more expensive option is to cluster the control room, associated support areas, the incident room and other security functions in a separate protected environment, where the security team remains even during rest periods and comfort breaks. This can enable faster response and communication during an incident.

ACCESS SHOULD BE VIA AN ELECTRONIC ACCESS CONTROL SYSTEM.

It's easy to defeat visual pass checking – the security guard can't know for sure whether the pass holder is still employed or authorised to access the control room area.

WHO COMES INTO THE CONTROL ROOM?

Here are three key things to bear in mind when you plan the policy for access to the control room:

- You'll probably need a **signing-in book**. (Check with your legal team – you'll hold personally identifiable information, so you'll need to comply with the Data Protection Act.)
- **Limit the number of people who have access to the control room.** The everyday access will obviously have to include the security guards who work there. Bear in mind that during an incident, if more people are in the control room they risk distracting the security guards from doing their job.
- If possible, during an incident **move the people who are focused on the strategic overview to an incident room**, so that they are not distracting the security guards.












WHAT ABOUT BIOMETRICS?

If you use biometrics as a second/third factor authentication for access to the control room, this must raise the levels of assurance that it's the authorised person (rather than the authorised card) who is entering the control room. Done poorly, adding biometrics could even reduce security!

You might want to zone working areas to show the level of security clearance needed – perhaps colour coding the floors and the passes: for example, red = SCR authorised list / prox and pin; amber = facilities / prox and pin; green = rest of site / wear pass only.

MORE INFORMATION

- **CPNI Biometrics Guidance** (CPNI, YouTube)

-
-  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Location of your control room](#)
 -  You may also want to read about [Windows, lighting and temperature](#)
 -  You may also want to read about [Room layout](#)
 -  You may also want to read about [Network security](#)
 -  You may also want to read about [Resilience](#)
 -  You may also want to read about [Visitors to the control room: overview](#)
 -  You may also want to read about [Access to the control room](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Incident rooms

What should your incident room include? It's a good idea to have input at the design stage from the people who are going to use it. You may need several incident rooms, each with its own purpose.

The room(s) should be included in incident practice as a matter of course. This will help ensure that the right equipment is there, and that it is designed in a way that does not disturb the core team. If you practise realistic day-to-day incidents, as well as incidents that would be high impact but are less likely, your team will be better prepared for the real thing.

LOW LEVEL AND FAST-PACED INCIDENTS

Usually the control room will deal with low level incidents, monitored by the supervisor, and there will be no need to set up a dedicated incident room.

The initial stages of a fast moving event will also be managed in the control room – this can mean that the control room becomes very busy and crowded. To avoid this, you may want to brief senior managers beforehand not to go to the control room during an incident: in this case it will be vital to ensure an effective flow of essential information to senior managers during an incident.

As a rule, it's best to discuss an ongoing incident away from the continuing work of the core team, to avoid disturbing them.

ESCALATION OF AN INCIDENT

It doesn't have to be a major incident to be dealt with by the incident room, and it doesn't necessarily have to involve high-level personnel. It is simply a practical way to ensure that the everyday business of the control room can continue efficiently.

Your incident room should be up and running as soon as possible after an incident is escalated.

Control of the incident will then pass to the incident room team (this may include people from outside agencies) which will allow the control room to go back to normal operations, maintaining the ongoing security of your site.

The incident room should hold lists of individuals who may need to be contacted in the case of an incident. This may add efficiency to the management of the incident once it occurs.

A STRATEGIC INCIDENT ROOM

During major incidents you may need a board-level strategic incident room, where strategic decisions are made that set direction and policy, as well as liaison with the media.

All incident rooms will need feeds in and out to keep in touch with the latest information on the incident. They will also need to liaise with each other and with external agencies.











It's important to identify the inputs and intelligence feeds required for each level of incident room and to exercise these.

If you keep the technology consistent across different levels of incident room, this makes it more straightforward for people to move between rooms as needed.

Remember:

- **People need regular practice with any unfamiliar kit** before they have to use it during an incident.
- **All equipment should be tested regularly** to ensure that it is fit for purpose, and that the software is up to date.

Different rooms will need different amounts and types of data, and your plan should include ways to ensure that this information is secure, up to date and clearly displayed. You may find video walls and news programmes useful in the incident rooms.

-
-  You may also want to read about [Location of your control room](#)
 -  You may also want to read about [How secure does your control room need to be?](#)
 -  You may also want to read about [Technical integration: overview](#)
 -  You may also want to read about [Network function](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Verification: overview](#)
 -  You may also want to read about [Escalation: overview](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Rest areas

WHAT MAKES A GOOD REST AREA?







Ideally it should be a room should be located away from the control room, so that when you take a break you can relax properly.

No TV. You may be surprised by that! But it makes sense – you spend a lot of time watching monitors, so what you really need is a screen break.

A quiet space – for some people it's important to have a bit of peace, free of conversation.

With a nearby toilet for comfort breaks, as recommended by HSE.

With appropriate comms – if necessary, the control room needs to be able to get you back on duty..

-
-  You may also want to read about [Location of your control room](#)
 -  You may also want to read about [How secure does your control room need to be?](#)
 -  You may also want to read about [Staff welfare at work](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Room layout

Effective communication is a key part of a well-run control room. And that starts with the layout – people can't see round corners in an L-shaped room, or see through pillars! **Aim for an open layout with clear lines of sight.**

It's a good idea to start by reviewing existing processes – a user interaction study will help you to understand communication paths and critical interactions.

If your control room needs windows, consider applying specialist films that obscure the view from outside and protect the information within, while allowing good lighting inside.

Depending on your assessment of likely threats to your site, you may decide that your control room should not have windows.

Consider carefully where the supervisors will work – the traditional position at the back of the control room is not necessarily best except when managing an incident. Communication generally improves where the supervisor is in the middle of the control room and the distance to all desks is minimised.

Any equipment that is only used from time to time can be located in a separate secure room. This has the added advantage of reducing the noise and heat in the control room.

Bear in mind that the control room is likely to be working 24/7, so maintenance or equipment replacement will probably happen while the control room is operating. For this to happen without causing major disruption, you'll need to allow sufficient access and space for large equipment to be moved in and out.


CCTV monitoring is best done primarily on desktop monitors where each security guard can review images without discomfort.


A video wall is not the primary tool for detection – it should only be used as a supplementary tool for incident management or supervisor overview. It's important that a video wall does not distract security officers from their main task. If they need to monitor an image on the video wall it should be transferred to a workstation display to avoid discomfort.


ACCESS POINTS


Consider the entry points to the control room. Nobody should be able to enter the control room directly from public areas such as the site reception. When someone enters the control room, passers-by should not be able to see what the security officers are doing or view CCTV displays.


Of course you'll need to consider how the control room will work when it's 'business as usual' (BAU) and during an incident. You may want to consider setting up a separate incident room. Where that is not an option, the control room will need to cover both BAU and the incident response (which may mean a sudden influx of people including senior managers to lead the response).


 You may also want to read about [Windows, lighting and temperature](#)


 You may also want to read about [Desk layout](#)

 You may also want to read about [Screen display](#)

 You may also want to read about [Incident rooms](#)


 You may also want to read about [Rest areas](#)

 You may also want to read about [Other control room functions](#)

 You may also want to read about [Effective communications](#)

 Go to [2. Design and build](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Desk layout

Some basic principles for a good office working environment are the same for a control room:

- Everyone needs to know how to adjust their chairs (especially important for security officers who may sit at their desk for long periods).
- Surfaces should be non-reflective to reduce visual fatigue.
- People should be able to adjust their desk to the height they need – this might mean the desk being adjusted when a new person comes on shift.
- Lighting should suit the task: people will need more light for written work, lower lighting levels for viewing monitors.

But there are some principles that are specific to control rooms. **Work out the primary and secondary roles for each desk, and tailor it accordingly.** A workstation used for CCTV monitoring should have a different layout from a desk used for writing tasks such as logging.

A security officer monitoring CCTV needs the screen significantly further away than someone working on word processing.

With the CCTV display too far away, the security officer might miss an important detail in an image.

If the display is too close, they will not be able to see all the display properly – the outer part of the image will be in their peripheral vision.

As a rule, you should position the display at a distance that's equivalent to 3 to 5 times the screen diagonal. That means a 20 inch (0.5m) display should be 60 to 100 inches (1.5-2.5m) from the operator.

It's important that the person at the desk can easily reach the computer peripherals they need to use for the task. Consider whether a joystick and buttons are better tools than a keyboard and mouse.

Wherever practical, **keep non-essential computer equipment off the desk** (for example, computer base stations should be away from the hands and feet of the person at the desk) and preferably out of the central control room area.

As well as keyboard and mouse, consider whether the people on your team need other tools such as function keys, touch screen, joystick, control panel (with buttons), voice-activated software, auditory feedback (eg a button beeping in response to an input) or haptic feedback (a device vibrating in response to an input).

i You may also want to read about [Monitoring CCTV](#)


i You may also want to read about [Screen display](#)

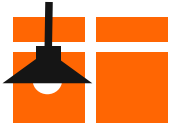
i You may also want to read about [Visual inputs](#)

i You may also want to read about [Map essentials](#)

 Go to [2. Design and build](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Windows, lighting and temperature

PEOPLE ARE YOUR MAIN ASSET

When you're designing a control room you'll need to balance its main purpose – security – with the needs and comfort of the people who work there.

Generally you'll want to make sure that people outside can't see what's going on inside the control room. On the other hand, people are often happier working if they can see out.

If your control room needs windows, consider applying specialist films that obscure the view from outside and protect the information within, while allowing good lighting inside. Depending on your assessment of likely threats to your site, you may decide that your control room should not have windows.

It's important that screens and work surfaces don't reflect light as this can increase eye strain and could lead to security officers making errors.

EVERYONE'S IDEA OF 'THE RIGHT TEMPERATURE' IS DIFFERENT









Room temperature is important.

- Get it right and you help people to work at their best.
- If it's too warm, they might struggle to stay awake.
- If it's too cold, their sensitivity to touch can be affected.

You'll probably find that people don't all agree about what is good lighting, or what's a pleasant temperature in the office. (In general women are more likely to notice sudden temperature changes and prefer a warmer workspace than men. People need different light levels when they are monitoring CCTV or reading paperwork, for example, or if they are older.) So it's a good idea to enable people adjust the temperature and the lighting for their workstation.

FURTHER READING

- **Fenestration Obscuration Guidance (how to obscure your windows)**
- **CPNI Guide to Security Lighting**

-
-  You may also want to read about [Room layout](#)
 -  You may also want to read about [Desk layout](#)
 -  You may also want to read about [Screen display](#)
 -  You may also want to read about [Staff welfare at work](#)
 -  You may also want to read about [How secure does your control room need to be?](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



CCTV operation

The purpose of your site's CCTV should be clearly defined and documented. This will inform your control room's operational requirement (OR) and the way the control room operates. It's also a legal requirement.

You'll probably have CCTV in order to achieve one or more of these aims:

- To detect an intruder as early as possible.
- To verify an alarm from a Perimeter Intruder Detection System (PIDS)
- To support security officer(s) or a security force
- To use with video analytics to classify activity

AS HUMANS WE NEED MINIMUM IMAGE SIZES, HOWEVER GOOD THE PICTURE QUALITY

- To **detect** an intruder, the target image must be at least **10%** of screen height.
- To **recognise** someone, their image needs to be **50%** of screen height.
- To **identify** someone, their image needs to be **100%** of screen height.

Where the security officer's CCTV display is a 'quad' screen (showing four images stacked two-high, two-deep) on one monitor, this reduces each image to half the height of a full screen. For detection, the target image will need to be at least 20% of the full screen height.

Each camera image should be actively viewed at least once every FIVE minutes to maintain full security of the site if its perimeter is protected by other physical security measures such as PIDS or fencing.

In some cases you'll need to view the images more frequently – this could be due to operational business needs, or where you are monitoring particularly busy or cluttered scenes or vulnerable points.

If part of the perimeter is damaged, or an entrance point is poorly protected, it's worth considering increased CCTV surveillance of that area. It doesn't necessarily mean installing more cameras – simple but effective measures could be increasing frequency or time spent monitoring the area, keeping the area's screen constantly on display or using video analytics for the area.

Where detection analytics are combined with CCTV, when an alarm is activated the security officer's screen should immediately show recorded footage to show the area before and after the alarm was set off. This may help them to determine the cause of the alarm and any follow-up action. At the same time they should see a live view of the alarm area on their second monitor.

Where CCTV and detection analytics are used in a blank screen configuration, the monitor will only show an image when an alarm is triggered. Blank screen technology is not a complete solution to replace active monitoring (checking each camera's view once every five minutes),

There are good reasons for using fixed cameras for a perimeter security CCTV system.

1. Fixed cameras provide a known and consistent image.
2. They can be configured to work for each specific location's particular characteristics.
3. You can tailor the lighting to that position and the light levels there.









Pan Tilt Zoom (PTZ) cameras are versatile but have inherent weaknesses.

1. The security guard can use the camera to follow an intruder or zoom in on an alarm location.
2. As the focus moves, the security guard may be less sure of exactly where the camera is pointed.
3. The camera may be left pointing in the wrong position.
4. Someone with hostile intent could distract the security guard and get them to move the PTZ cameras so that an event is not spotted.

For the best security, you may want to combine fixed cameras to cover the perimeter with supplementary PTZ cameras to investigate or track an intruder.

Depending on the acceptable level of risk, **you'll need to consider how to cover blind spots where there is no camera coverage.** These should be known to everyone involved from security officers to managers, and covered by other methods such as patrolling security officers on the ground, or CCTV patrol with a PTZ camera.

Note: if your CCTV monitors a public space, you must hold an SIA public space licence. There are certain exemptions, for example, if CCTV is solely there to identify trespassers or if there are in-house guards.

-
-  You may also want to read about [Monitoring CCTV](#)
 -  You may also want to read about [Screen display](#)
 -  You may also want to read about [User interface layout](#)
 -  You may also want to read about [Detection analytics](#)
 -  You may also want to read about [Visual inputs](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Monitoring CCTV

How many images can you expect a security officer to check over a 5-minute period? That will depend on where the CCTV cameras are located.









If someone has hostile intentions they will almost certainly prepare for an attack by carrying out hostile reconnaissance beforehand, and they will be looking for the most vulnerable areas.

The tables below summarise maximum number of images you can expect an operator to review in various situations to comply with that 5 minute review rule, when they are monitoring fence lines or monitoring crowded areas.

Bear in mind that if a security officer is covering the maximum number of images, they should not have other tasks to complete at the same time such as critical site operations or first aid while monitoring CCTV.

What is it covering?	Fixed camera image	PTZ (Pan-Tilt-Zoom) camera images
Fence line with PIDS* looking at an area or location that is sterile (nothing should be happening) or relatively inactive; where there are no dedicated eyes-on security officers	50	35
Fence line without PIDS , active monitoring in busy or vulnerable areas where there are no dedicated eyes-on security officers	15	10
Fence line active monitoring looking at an area or location that is sterile (nothing should be happening) or relatively inactive; where there are no dedicated eyes-on security officers	20	15
Fence line secondary assist role to support ground positioned staff	30	20
Primary monitoring of crowded areas (e.g. shopping centres) for hostile acts, suspicious items etc. with no dedicated guard force. (Note: crowded areas are only crowded at specific times – not 24/7)		5-10 depending on scene
Secondary role for monitoring of crowded areas (e.g. shopping centres) for hostile acts, suspicious items etc. to assist dedicated ground staff (Note: crowded areas are only crowded at specific times – not 24/7)		10-15

* PIDS perimeter intrusion detection system

-
-  You may also want to read about [CCTV operation](#)
 -  You may also want to read about [Desk layout](#)
 -  You may also want to read about [Screen display](#)
 -  You may also want to read about [Visual inputs](#)
 -  You may also want to read about [Shift lengths and task rotation](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Screen display

When it comes to the number of screens at a workstation in the control room, less is more. If you have to keep an eye on too many displays and CCTV images, the chances are you'll miss something significant.

The recommended setup for a desk in the control room has three screens: one for CCTV monitoring, the second to check alarms, access control or a Security Management System, and the third for reviewing recorded CCTV.

If the security guard has other general duties (such as emails or filling in time sheets) they will need to do these at a separate workstation, or at a time when someone else is responsible for monitoring CCTV.










It's important to think about the tasks that you want security officers to carry out, and to specify the displays according to those tasks. You'll need to do this at the planning stage (when you work out your operational requirement) and when you change equipment. For example, when you change the cameras on your site, you should review the whole CCTV system including displays.

A human cannot detect an intruder that is less than 10% screen height, no matter how good the quality of the image – they won't be able to see if it is a person, a car or an animal.

Avoid screens that 'upscale' images – if the display resolution does not match the resolution of the transmitted image, there may be visual anomalies that make it harder for the security officer to detect intruders.

A video wall is not the primary tool for detection – it should only be used as a supplementary tool for incident management or supervisor overview.

It's important that a video wall does not distract security officers from their main task. If they need to monitor an image on the video wall it should be transferred to a workstation display to avoid discomfort.

-
-  You may also want to read about [Desk layout](#)
 -  You may also want to read about [User interface layout](#)
 -  You may also want to read about [Monitoring CCTV](#)
 -  You may also want to read about [CCTV operation](#)
 -  You may also want to read about [Visual inputs](#)
 -  You may also want to read about [Visual warnings: overview](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Visual inputs

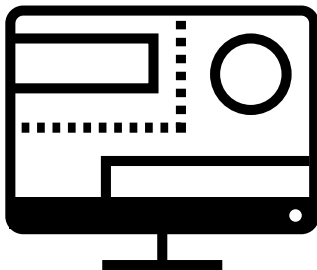
IT'S IMPORTANT NOT TO OVERLOAD PEOPLE WHO ARE MONITORING SCREENS

But you will need to consider some logistical factors:

1. If you're trying to watch too many screens or too many CCTV feeds at one time, it's harder to detect an event.
2. If you have a video wall, take care that it doesn't distract security officers from their main focus – monitoring CCTV on their desktops.
3. **Desk displays should only be used for primary duties.** Other tasks, such as email or timesheets, are best done at a separate workstation.
4. You need regular screen-breaks to help reduce visual fatigue.
5. Screen refresh rates below 50Hz tend to flicker. This can cause eye strain, so higher rates are advisable.

WHAT'S ON THE DESK?

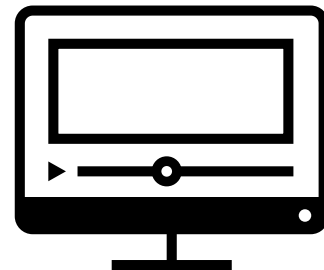
In most cases, three screens on a desk are the recommended maximum:



CCTV monitoring



Alarms from detectors













Reviewing recorded CCTV

The viewing angle of the screens and the distance the viewer sits away from the screens both need to be adjustable so that each person can work at their best.

Video walls are best used for incident management and overview – it can cause discomfort if you have to view images there for long periods. If you need to monitor a particular image from the wall, it's best to transfer it to a CCTV monitoring desk.

FURTHER READING

- [HSE guidelines on Seating at Work](#)
- [HSE guidelines on Display Screens](#)

-
-  You may also want to read about [Monitoring CCTV](#)
 -  You may also want to read about [Screen display](#)
 -  You may also want to read about [Desk layout](#)
 -  You may also want to read about [User interface layout](#)
 -  You may also want to read about [Detection analytics](#)
 -  You may also want to read about [Visual warnings: overview](#)
 -  You may also want to read about [Auditory alarms: overview](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



User interface layout

The user interface is where the user ‘meets’ or interacts with the information. It can be anything from a simple paper-based system (a CCTV monitor, a paper log book and an alarm panel) to a fully integrated Security Management System (SMS) with computed mapping.

The way information is supplied and shown to the security officer is critical. If it's well designed, the user interface can make the everyday control room more efficient and improve the response when there is an incident through:

- Better situational awareness
- Better detection
- Faster response to a situation
- Better tailored response to a situation.

FIVE TOP TIPS THAT APPLY WHETHER YOUR USER INTERFACE IS SIMPLE OR SOPHISTICATED

- Keep maps simple and consistent in style.
- Users need to be able to log incidents as free text (in a paper logbook or a text file on screen).
- A set of example camera views helps the security guard compare each one with live footage and check that each camera is still covering the right area.
- Additional text information about each camera view can give a security officer essential details about the area covered by the camera they are monitoring.
- Security officers tracking an incident will be able to respond faster if they can access additional information about the area covered and other cameras offering views.

It's also worth adding Standard Operating Procedures (SOPs) and response information to the interface so that security officers know where to find the information quickly to help them deal with incidents quickly and correctly. (On an integrated SMS this information may be accessed on a second screen alongside the main CCTV monitor, while a security officer using a paper-based system would find the information on printed information sheets.)

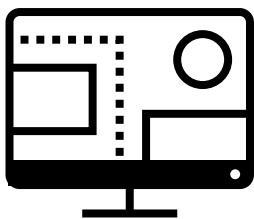
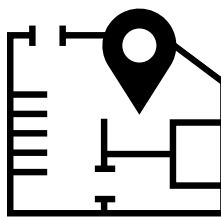



Image on screen




Map with location pinpointed




Supporting info

 You may also want to read about [Monitoring CCTV](#)

 You may also want to read about [Screen display](#)

 Go to [2. Design and build](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Network security

Your IT network security is absolutely critical to your operation. It's important to have a specific IT policy that applies to the security system – in some aspects this will be more stringent than the wider corporate IT security policy and it may require more advanced functionality.

The highest level of physical security IT network is independent of any other network or system and has not external connections outside the protected area. (For more details see CPNI Cyber Assurance of Physical Security Systems CAPSS Guidance.)

If your physical security system uses IP connectivity with engineering remote access mode, this may use identifiable account credentials. It's a good idea to replace any default accounts with custom accounts; if some core accounts cannot be removed, be sure to set up a secure password.

MAINTENANCE

The way engineers access your IT system can make the system more vulnerable. If they log in remotely (usually much cheaper than deploying an engineer to the site) to fix problems and offer first line maintenance, this could be an opportunity for someone with hostile intent to acquire a trusted login and a very powerful account. If it's impractical to disable a remote engineer login, it's a good idea to restrict the login rights to viewing logs, and to ensure engineers are not permitted to change settings, read or write to personal data or perform any other functions on the network.

Updating and patching of the security infrastructure should be overseen by both IT experts and security experts, and it's essential to keep accurate records. Updates should always be tested in a test environment before being applied to the live system.

When installing manufacturer's updates, be sure to monitor the import carefully and use the virus checker. (Manufacturer or integrators often use the same laptop or USB device to update at multiple sites with varying levels of IT security – this could potentially transfer a virus to your security network.)

BACKING UP YOUR FILES

While it makes sense to allow a third party to hold a backup copy of your site's generic software implementation, site specific keys should only be held on site, not by a third party.

Your absolute priority, when keeping your backup key information secure, is to ensure it's not accessible to third parties.









Backup security should apply to items such as electronic key / lock information, passwords to software logins (eg for security management systems), automated access control system card information, site keys and personal data, intrusion detection system access information, encryption details and so on.

EXPORTING DATA

Your IT security policy should cover procedures for exporting CCTV clips or data to external parties, such as the police.

It's essential to control any media that is connected to the physical security system to reduce the risk of introducing unauthorised software or malware onto the system. If data has to be downloaded from the system it is advisable to use a new USB drive or a new removable disk each time for this purpose. Any peripherals such as USB ports that are not required should be disabled or removed.

You may want your control room to have access to the internet for news, intelligence and maps. Internet use should follow company policy. For maximum security the internet connection could be restricted to a standalone machine that is physically separate from the security network.

-
-  You may also want to read about [Network function](#)
 -  You may also want to read about [How secure does your control room need to be?](#)
 -  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Data retention](#)
 -  You may also want to read about [Maintenance and repair](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Network function

A well run physical security system, run over IT infrastructure, requires specialist skills in both IT and physical security. Ideally:

1. The security team defines what they require of the network.
2. The organisation's IT department delivers it.
3. The IT department and the security team work together to manage the security network and systems.

Depending on the systems run over the IT network, substantial bandwidth will be required to run the security systems. Alarm and notification systems mostly run on fixed bandwidth, but for CCTV it can vary widely, depending on compression, resolution of the images, and frame rate of the footage.

REDUCING BANDWIDTH

You may find that you are asked to reduce the security bandwidth. In that situation **each of these functions will need to be carefully balanced to ensure that the images viewed in the control room are fit for purpose.**

Compression (reducing the file size) – generally speaking, higher compression needs lower bandwidth, but means lower picture quality. 'Lossless' compression (very few techniques are truly lossless) reduces the bandwidth with little effect on picture quality. 'Lossy' compression reduces the size of the picture but reduces picture quality as well.

- Resolution (the number of pixels in an image) – more pixels, the better quality image, and the greater your ability to zoom in and see detail. High resolution images are better quality but need greater bandwidth.
- Frame rate (the number of still images per second in a video). The human eye interprets 25 frames per second (FPS) as moving images, and this is the recommended frame rate. You can reduce the FPS to lower the bandwidth required but some of the action within the scene will be lost. If a CCTV camera takes 1 picture every second it may not capture an image if someone crosses the area it covers in less than 1 second. Very little contextual information is captured from 1 image a second – even if you see the target they may be facing away from the camera.

TOO MUCH DATA CAN CAUSE THE SYSTEM TO CRASH

If the system is trying to transmit more data than the bandwidth can cope with, it will result in bandwidth lag: data in the network backs up and takes longer to transmit. This may only mean a minor delay on alarm notifications but where CCTV data is continuous and the system is overloaded the network may crash or even cause data to be deleted.

A network running close to capacity will show lag on the control of Pan Tilt Zoom (PTZ) cameras, with slow response when a camera is moved, and less precise manoeuvring. This can seriously affect the capacity of security officers to find and track objects within the scene.

IT NETWORK SUPPORT










Security is a 24/7 operation. Ideally the IT support infrastructure needs to be available 24/7 too, so that any problem with the server or other equipment in the middle of the night can be fixed promptly and good security maintained.

If your security department has to manage the installation and support of the security IT network, these are the main items to consider.

- Monitoring
- Storage / back-up
- Data centre management
- Data transfer
- Privileged access
- Active directory
- Service level agreements
- Networks
- Servers
- Workstations
- Patching / service packs
- Antivirus
- Removable media controls
- Development environment
- Unsupported systems
- Patching

IT COSTS

When you're looking at the costs for IT, you should generally assume that any part of the IT infrastructure will need to be replaced or renewed every five years. As well as staff costs and any support contract, you'll need to cover the cost of software user licences, monitoring software, development environments, test beds and admin costs.

-
-  You may also want to read about [Monitoring CCTV](#)
 -  You may also want to read about [Screen display](#)
 -  You may also want to read about [Technical integration](#)
 -  You may also want to read about [Network security](#)
 -  You may also want to read about [Data retention](#)
 -  You may also want to read about [Maintenance and repair](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Detection analytics

Your Operational Requirement (OR) Level 1 will set out the level of detection required for your site. It's essential that you use this to clarify the kind of detection system you require and the specific purpose of that system.

You'll probably want to automatically alert security guards if there is an alarm. That first alert can be activated by automated analytics (detection system): the human security guard will need to decide which alerts need to be followed up.

DETECTION TECHNOLOGIES PROS AND CONS

Detection systems are good at covering well defined areas – a perimeter wall or a door, for example – and for specific tasks. Unlike humans, they work 24/7, they don't lose concentration when they get tired, and don't need rest breaks. But humans are much better at analysing complex scenes, and interpreting what's going on.

Any detection system installation has to balance two key measures that are interdependent:

- 1. To maximise detection rate you increase the sensitivity of a detection system.**
- 2. To minimise false alarm rate you decrease the sensitivity of a detection system.**

In the ideal world you'd be able to detect 100% of attacks. A more realistic target might be 95%, though your site may be OK with a lower figure.

And in the ideal world there would be no false alarms! But depending on the size and scope of your site, and how many people you have patrolling the perimeter, a more realistic daily target might be 5-10 per kilometre of fence, for example. Many more than that and you may find that people start to ignore the alarms.

VIDEO DETECTION ANALYTICS

Video analytics (often referred to as video based detection systems, motion detection, or video content analysis) uses a computer system to monitor and look for changes or patterns within a CCTV image. When this is detected, the system alerts the security guard in the control room.

It can include:

- **Real time monitoring** to trigger or increase recording. The system will only record behaviours it is trained to recognise, so other behaviours may be missed or recorded at a lower quality.
- **Identifying events for a human to interpret.** 'Black screen technology' that only shows an image on the security guard's screen when video analytics system defines as being of interest
- **Analysing events and generating alarms for a response**
- **Acting as a PIDS** (perimeter detection intrusion system) and filtering pre-recorded footage after an incident

While the system is being set up each video channel (camera view) will be individually tuned, and it's normal to see a higher number of false alarms.

INTRUDER ALARM ANALYTICS












Intruder alarm analytics are mostly used as part of Perimeter Intruder Detections Systems (PIDS). These systems use sensor wires attached to perimeter fences to detect a potential attack. The system analyses the sensor signals to work out if they are indicating an attack. This is only useful for real-time monitoring but can be effective, enabling one security officer to monitor a greater area. Intruder alarm analytics is not foolproof or comprehensive so alarms should be verified by CCTV.

AACS AND IT ANALYTICS

Analytics applied to other systems such as Automated Access Control Systems (AACS) or IT systems can identify patterns in people's work behaviours over a longer period. They may be useful in spotting security concerns when people access buildings or IT systems out of usual hours.

FURTHER READING

- **CPNI Testing installed video analytics guidance**

-
-  You may also want to read about [CCTV operation](#)
 -  You may also want to read about [Network security](#)
 -  You may also want to read about [Personally identifiable information: internal review](#)
 -  You may also want to read about [Personally identifiable information: external review](#)
 -  You may also want to read about [Visual inputs](#)
 -  You may also want to read about [Visual warnings: overview](#)
 -  You may also want to read about [Auditory alarms: overview](#)
 -  You may also want to read about [Escalation: overview](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Data retention

Your site should have a clear written policy on the retention of data and personally identifiable data. This policy document should cover security, privacy and other relevant regulations (for example, financial institutions are required to keep logs of some data for seven years). The policy document will be subject to review by the Information Commissioner's Office. If your site is a public body, it may be subject to Freedom of Information requests.

The data retention policy document should be based on the Operational Requirement (OR) for the system and its use. It should define uses of the system, the purpose of the data collected at your site and the maximum period data is required to be kept.

DEPENDING ON THE PURPOSE, THE TERMS OF DATA RETENTION WILL VARY

- If the system is designed to protect against terrorism and mass casualty events, the recording could be deleted 24 hours after recording
- If the system is designed to capture long term hostile reconnaissance, the retention period may be 30 days or longer.
- Shorter retention periods may mean that other matters such as low level crime are missed, but if the system is not designed to capture that, it would be against the data retention policy.

Any CCTV imagery that is retained should conform to the CCTV code of practice. This will help with end user assurance and should assist with implementing a fit for purpose systems

12 GUIDING PRINCIPLES FOR CCTV SYSTEM OPERATORS








The Home Office's Surveillance Code of Practice spells makes the following recommendations.

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Once data is no longer required, it should be destroyed appropriately – it should not be stored just because you have the space to store it. This will usually mean that old data is overwritten with new data. It's important that the overwriting function is checked regularly and your site is confident that data is not being kept longer than the time specified in the site's data retention policy.

Your policy on data handover should differentiate between passing data to internal departments (where the security department will be able to follow up and check that the data has been destroyed) or to external people/organisations, where the site is unlikely to be able to verify its destruction.

-
-  You may also want to read about [Monitoring CCTV](#)
 -  You may also want to read about [Network security](#)
 -  You may also want to read about [Personally identifiable information: internal review](#)
 -  You may also want to read about [Personally identifiable information: external review](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Personally identifiable information: internal review

Personally identifiable information will be captured in CCTV footage, AACS logs, IDS logs (which could show someone's daily habits) or other information.

Your site should have a policy document setting out the circumstances in which personally identifiable information may be requested for review by a person working at the site. This could be for security issues, discipline issues or other legal reasons.

If there are instances where CCTV may be used other than for its stated purpose, this should be noted as a condition of employment or condition of entry onto site and should be clearly stated to all employees and visitors. If this is a condition of employment, careful consideration needs to be given to visitors and other non-employees.









Any access to personally identifiable information should be logged.

The location where personally identifiable information is reviewed should be carefully considered to avoid distracting the other security officers from their main duties. For potentially sensitive cases, or where it is essential to restrict the viewing to specific people, it may be best to review the personally identifiable information in a private office. Take care that this does not lead to unauthorised viewing of personally identifiable information or breach the data protection policy.

It will be important to have the option of saving data for investigation: this would mean overriding any auto-delete or auto-overwrite functions, but ensuring that a robust policy is in place to ensure the data is duly destroyed after its required use.

DATE AND TIME STAMPS

An important aid when reviewing CCTV is the date and time stamp to pinpoint when an event takes place. You may want to show the time zone as well, for example 22:15 (GMT) or 23:15 (GMT+1).

-
-  You may also want to read about [Personally identifiable information: external review](#)
 -  You may also want to read about [Room layout](#)
 -  You may also want to read about [Network security](#)
 -  You may also want to read about [Data retention](#)
 -  You may also want to read about [Resilience](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Personally identifiable information: external review

Whenever data is requested by people or organisations outside your organisation, it's important to establish that this request is legitimate. Personally identifiable information will be captured in CCTV footage, AACS logs, IDS logs (which could show someone's daily habits) or other information.

In some instances a court may require you to provide personally identifiable information or footage. You'll need to consider the implications, as well as what may be revealed if the court then orders that information or footage to be released.

If you hand over data to an outside organisation, always include instructions on how it should be stored and, most importantly, how it should be destroyed.

Any transfer or copying of data should be logged by the control room; if correct instructions have been passed on to the recipient, you should assume that the data will be destroyed accordingly.

DATE AND TIME STAMPS








The date and time stamp is an important aid when reviewing CCTV - it pinpoints when an event takes place. You may want to show the time zone as well, for example 22:15 (GMT) or 23:15 (GMT+1).

When information is reviewed by external agencies the information should be given across in a standard easily readable format (not as a proprietary encoded video file).

If it is appropriate you may also be required to supply other information from your site about an event, for example, control room logs or eye witness accounts. In this case you are advised to provide copies rather than the original files, and to log the action accordingly.

FILE FORMAT

If you are required to hand over data for external review, you will need to provide it in an easily readable format, preferably open-source.

-
-  You may also want to read about [Personally identifiable information: internal review](#)
 -  You may also want to read about [Room layout](#)
 -  You may also want to read about [Network security](#)
 -  You may also want to read about [Data retention](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Resilience

Building resilience can be costly: in most cases the backup control room will rarely be used. But when you consider what the loss of the main control room would mean – major disruption to the site and significant costs in terms of staff time and equipment – it's essential.

If you're a security manager, you'll need to work out the level of resilience your site requires, and mitigate risks to a level that you consider acceptable.

The control room is the first level of resilience. If the integrated system fails, you'll need to ensure that the control room can fall back to individual systems or to manual methods. This could mean accessing a standalone CCTV viewing area, being able to monitor IDS and PIDS panels, and manually logging in a book.

It's important that everyone on the team is trained on these fall-back systems and practises using them, otherwise valuable time will be lost at a critical time when an integrated system is down.

Where external factors pose significant difficulties, your control room should be resilient enough to keep running. For example:

1. **Power cuts** – your control room needs a backup power supply.
2. **Extreme weather** – it's important to protect against flooding and other weather events.
3. **Loss of heating or air conditioning and other environmental problems** – this could be simple responses such as providing extra clothing or water supplies.
4. **Staff shortages** – where there aren't enough people available, control room managers should be able to call on extra staff or call in additional staff from outside the organisation (such as contract staff or from another organisation on a staff share agreement).

You can design in resilience by providing two control rooms: **the primary control room** for use under normal operating conditions and **a secondary backup control room** for use in the event of a failure. To maximise the value of the secondary control room (which may otherwise considered an expensive duplication) it could be used as the incident room unless the primary control room is unavailable.

Ideally the primary and secondary control rooms are interchangeable, with duplicated security capabilities including CCTV feeds and hardware, IDS alarms, access control, all supporting infrastructure and IT. Both control rooms should be tested and regularly maintained to the same standard.

It's important to test the effects of a power cut on both primary and secondary control rooms, to ensure that moving to the backup power supply causes minimal disruption to the control room and its systems, as well as security systems around the site.

It's a good idea to test various scenarios such as power failure to the control room, security management system failure, and individual system failure (such as intrusion detection systems, access control, lighting). Testing should include moving to the backup system and any alternative actions such as deploying security officers to the perimeter.

If your site needs to be highly resilient, you may need to employ an on-site specialist maintenance engineer for the security systems and associated infrastructure.

If an on-site specialist maintenance engineer isn't appropriate, you'll need to set up a service level agreement with your supplier (including callout times) and consider other ways to cope when the control room is down, such as having a secondary control room and holding critical spares on site for rapid repairs.

If your secondary control room is located off-site, it can give added resilience against terrorist threats or natural disasters. But you will need to consider some logistical factors:












- Will there be trained staff in both primary and secondary control rooms during an incident? How will your trained staff get between the two locations?
- If you use contracted-out control room staff, is the response guaranteed? Will you be competing with other companies for the staff resources?
- Is your secondary control room sufficiently resilient if it is also affected by the same incident, such as localised flooding?

The design of your primary and secondary control rooms should be consistent. People who work there should use both control rooms regularly to get to know the setup and test the equipment. This helps to reduce the chance of security officers making errors under pressure when they switch from one control room to the other.

In both primary and secondary control rooms, it's important to have a secure method to deactivate the other control room. This may be needed during an incident or where the other control room is overrun. However it's important to secure the 'legitimate' control room so that it cannot be deactivated by an overrun control room.

FURTHER READING

- **CPNI CCTV best practice guide**

-
-  You may also want to read about [Network function](#)
 -  You may also want to read about [Network security](#)
 -  You may also want to read about [Security officers](#)
 -  You may also want to read about [Location of your control room](#)
 -  You may also want to read about [Maintenance and repair](#)
 -  You may also want to read about [Shift lengths and task rotation](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Exercises and simulations: overview](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Technical integration

Integration can have significant impact: it can increase the effectiveness of a control room and minimise the time needed to verify and respond to an incident. It can range from the basic (such as using the same number for a PIDS zone and the camera view that covers it) to a full-scale Security Management System (SMS):.

You can integrate (link) technical security measures at different levels:

- locally at the component level
- locally at the node (such as swipe card controls)
- centrally at the SMS control, for example such as Automated Access Control Systems (AACS) for large sites or PIDS activated blank screen CCTV.

When you integrate systems, make sure you don't end up with all the security on a single point of failure.

It's a good idea to ask these questions:

- Are there any unintended effects of integration?
- If the integration fails, can the technology fall back to individual systems?
- If you join two systems, what are the weak points?
- Where / how would someone with hostile intent be able to get access?
- If you integrate non-security systems, such as building management systems (BMS), will vulnerabilities increase?

Technical integration can be very positive in increasing detection rates and reducing workload for the security officers. For example, linking CCTV to PIDS/IDS using alarm-activated blank screen technology could help draw the security officer's attention to an event and improve the detection rate. **But it's not a good idea to rely completely on technology – human detection and understanding are essential.**


Integration can also help technologies work better together but you need to consider whether the outcome is what you want. Similarly it's important to consider the implications when one system depends on another.


Consider these scenarios:


1. You link CCTV to an automated access control system (AACS) to increase picture quality on CCTV recording when someone on registered on the AACS enters through a door. (Likely result: an attacker who is not registered on the AACS would not trigger the higher resolution image.)
2. You link a PIDS system to the perimeter security lighting, so security lights go on whenever a PIDS alarm is received. (Result: CCTV will have no useable pre-alarm footage as the site's perimeter will be in darkness until the alarm is triggered.)


But it's important to be aware that **integration may make your systems more vulnerable**. If one system malfunctions, this may prevent a linked technology working. It could mean that a person with hostile intent only needs to defeat one of the linked systems to beat the other part of the integrated system


If it is done correctly, further integration of security systems onto IP networks (linking systems across multiple sites) can have a massive security bonus and offer additional benefits for physical, personnel and cyber protection. Always consult the IT department and IT security specialists when planning large-scale integration or SMS linking IP systems across multiple sites.


 You may also want to read about [How secure does your control room need to be?](#)


 You may also want to read about [Network security](#)

 You may also want to read about [Resilience: overview](#)

 You may also want to read about [Visual inputs](#)


 You may also want to read about [Map essentials](#)

 You may also want to read about [Visual warnings: overview](#)

 You may also want to read about [Auditory alarms: overview](#)

 Go to [2. Design and build](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Maintenance and repair

When your security system needs maintenance, this will inevitably have an impact on the control room.

Unless the system is well maintained, you will experience increasing false alarms, but have reduced ability to verify alarms – and the security team's workload will increase.

Whether maintenance is proactive (ensuring regular maintenance checks are made) or reactive (waiting until something happens, compromising security and disrupting operations) will probably be down to your site's organisational policy.

PROACTIVE MAINTENANCE IS ALWAYS THE BETTER APPROACH

A well maintained security system will greatly reduce the workload of the control room and therefore increase the security of the site. **Maintenance issues should be logged as a security issue** and raised in a daily report.

ON-SITE OR ON CALL SUPPORT?

If possible, **it's an advantage to have on-site technicians / engineers who are familiar with the site and its security technology** and will understand the culture and risk appetite of the site. It can also mean that repairs are carried out faster.

On-call contract engineers may be cheaper but will probably only respond within the quoted time frame. **Where contract engineers are used, Service Level Agreements are essential** – this should include 'Time to repair' rather than 'Time to attend' (it's not enough for an engineer just to turn up, maybe without knowledge of the system and without the right parts). It's also worth specifying the service level outside office hours.

REPLACEMENT, REPAIR AND MAINTENANCE

One certainty is that any form of IT system will need replacement and maintenance. This will probably need a specialist resource from the organisation's IT department, so you'll need to have Service Level Agreements in place for this.

It's a good idea to hold any critical spares on site for rapid repair in case of failure. Security equipment is often bespoke or has long lead times for delivery of parts. Availability, reliability and maintainability factored into the design. You may need to have a back-up device in place for some products.

Be prepared: plan the replacement life cycle so you know which equipment is ageing or out of production and you can set aside budget to replace it.

Your security guards should not have to check lighting levels, top up washer fluid bottles or check PTZ (pan-tilt-zoom) motor heads – this kind of ongoing, cheap maintenance is better contracted to a dedicated department, allowing your security team to focus on their key tasks.

If maintenance work is likely to disrupt security operations, the control room should be notified and the event logged. When the work is completed the control room should be notified and confirm that the equipment is fully functional again – this would include checking camera positions and resetting alarms.

REGULAR CHECKS ARE IMPORTANT

Camera views should regularly be checked and audited to check that they still fulfil the intended use and cover the expected view (a screen shot of this view should be on file). This audit process should use the Rotakin test target.

It's important to check logs for automated systems such as AACS and IDS and examine them for anomalies. If any alarms have been inhibited, check them and clarify why.

Check daylight and night-time performance of equipment

The maintenance team should check that the security system and individual components are working correctly both in daylight and in darkness, and that they fulfil the Operations Requirement. This could be done by:










- reviewing CCTV from night-time
- reviewing CCTV from daylight hours
- reviewing historic logs
- performing physical checks in daylight and at night.

As well as the obvious maintenance tasks (fixing broken or empty items) the maintenance team should consider aspects such as lighting and colour rendition.

Bear in mind that over time, sensitivity of a detection system may be turned down to reduce the number of false alarms. It's important to check that the detection rate is still sufficiently high – simple attack trials will show whether that is the case.

FURTHER READING

- **CPNI Testing installed video analytics guidance**

-
-  You may also want to read about [CCTV operation](#)
 -  You may also want to read about [Technical integration: overview](#)
 -  You may also want to read about [Network function](#)
 -  You may also want to read about [Resilience: overview](#)
 -  You may also want to read about [Exercises and simulations: overview](#)
 -  You may also want to read about [Follow-up after exercises and incidents](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Monitoring the control room

As the control room is a working environment, it is normal to monitor it to check that it is working as effectively as possible. This should aim to maximise security – it should not be about maximising the number of tasks security officers have to complete.

Key Performance Indicators (KPIs) can be used to gain a quantitative understanding of the control room. These should be based on the Operations Requirement for the control room: they should focus on what the control room aims to achieve, rather than what it is doing now. For example, 'The control room should be detecting 95% of attacks on the fence' rather than 'Fence alarms should be resolved within 5 seconds.'

The control room Key Performance Indicators (KPIs) should be security specific. Other departments such as finance or human resources will have different requirements.












KPIs could cover items such as:

1. Number of alarms received and the actions from these alarms
2. % of operator time spent on any one task
3. Target response time to certain incidents (this will include exercises where the KPIs cover incidents that don't often occur)
4. Training undertaken
5. Replacement of control room systems
6. Maintenance repair times
7. Maintenance issues (such as non-functioning cameras)
8. Picture quality
9. Personnel (attendance, sick leave, holiday and so on)
10. Persistent problems

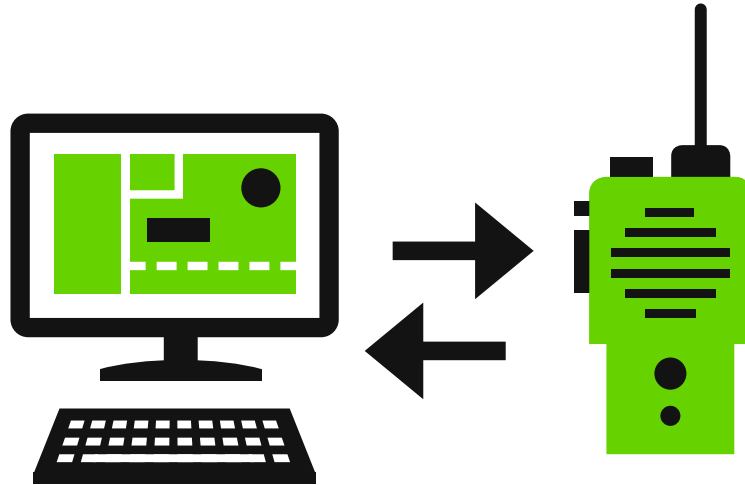
You should ensure that records are kept of performance monitoring of the control room and any outcomes for audit purposes.

FURTHER READING

- **Human Factors Checklist: Manager Survey**
- **Human Factors Checklist: Operator Survey**

-
-  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [CCTV operation](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Other control room functions](#)
 -  You may also want to read about [Access to the control room](#)
 -  You may also want to read about [Maintenance and repair](#)
 -  You may also want to read about [Staff training](#)
 -  You may also want to read about [Escalation: overview](#)
 -  Go to [2. Design and build](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)

Communications: overview



Good communication between security officers in the control room and on the ground is vital.

- It may increase the speed of response to a security incident.
- It can improve the chances of detaining an intruder.

Training is essential, so that everyone knows how to use radios effectively, and what the procedures are (especially if the usual communication tools aren't working). It's also very important that everyone uses the same names for places and assets on the site.

Everyone (supervisors, security officers in the control room and on the ground) needs to know:

- who communicates with whom during an incident
- how messages reach supervisors
- what backup procedures are if primary communications tools stop working.

-
- [i](#) Read more about [Effective communications](#)
 - [i](#) You may also want to read about [Room layout](#)
 - [i](#) You may also want to read about [Shift handovers](#)
 - [i](#) You may also want to read about [Roles and responsibilities](#)
 - [i](#) You may also want to read about [Response and decision-making criteria](#)
 - [Go to 3. Business as usual](#)
 - [Go to start of Control Rooms Guidance](#)
 - [Go to Glossary](#)

Maps: overview



In your control room you'll probably need one or more maps that are specific to your site.

Here are our top tips when you create a map:

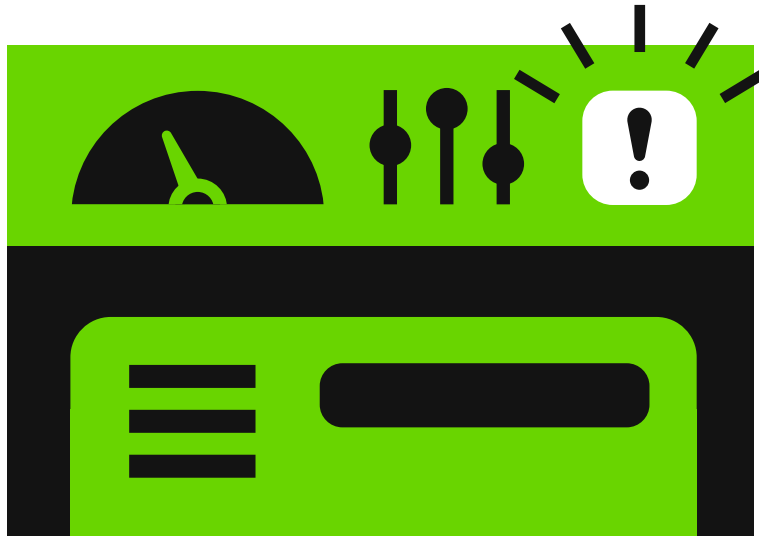
1. Keep it simple – restrict the detail to the essentials.
2. Show where North is (usually at the top of the map).
3. Use consistent points of reference and names for assets, places on site, roads and paths.
4. Make sure your map correlates with emergency plans.
5. Use a key (legend) to explain colours and symbols and a scale that people can relate to (eg 100 metres).

Always test your map with people from each group that's going to use it – their feedback can help improve it.

Make sure everyone uses the same version of each map, whether they are in the control room, on the ground or offsite.

-
- [!\[\]\(4f6d8a8b127300a02d56d34d01423d15_img.jpg\) Read more about Map essentials](#)
 - [!\[\]\(7e3d1ad67bf2d7a17700a66d1a313f91_img.jpg\) You may also want to read about Effective communications](#)
 - [!\[\]\(6aaf22e5a325c32ef2122c2939c64f9c_img.jpg\) You may also want to read about Incident response plan: overview](#)
 - [!\[\]\(27421322d686d4980ae2b7f101ee89ba_img.jpg\) You may also want to read about Evacuation plan: overview](#)
 - [!\[\]\(c45bffa8c48916027d3ccd561ed26723_img.jpg\) Go to 3. Business as usual](#)
 - [!\[\]\(bac5dbca87c84b327a183d989114aa0a_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(9b39af2adf53a7d5459150a09631e679_img.jpg\) Go to Glossary](#)

Visual warnings: overview




A visual warning that an alarm has gone off must attract the security guard's attention.


This kind of warning often fails because they are unclear, with complex text, and appear in unsuitable positions.

What should you do when you're creating a visual warning? Here are five tips:

1. Keep it simple.
2. Use simple, clear text.
3. Use symbols where you can – symbols get the message across faster than text.
4. Use red for the highest level of warning (everybody knows the traffic lights colour code).
5. If your warning is in black and white, make the words TWICE the size of warning text in colour.


 Read more about [Visual warnings](#)

 You may also want to read about [Auditory alarms: overview](#)

 You may also want to read about [Visual inputs](#)

 Go to [3. Business as usual](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)

Auditory alarms: overview



Alarms should cause alarm! They should be impossible to ignore.

There are often lots of false alarms in control rooms – security officers may tune out from the warning sound if they think it's probably a false alarm. If only one auditory alarm is used, people are more likely to miss the alarm or ignore it.

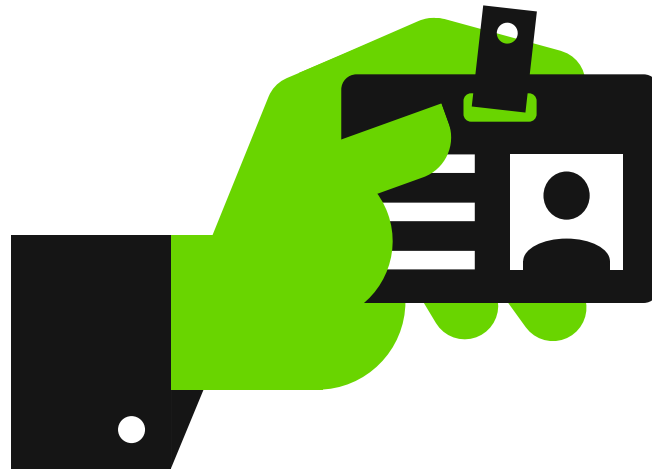
So here are some top tips for your auditory alarms:

1. The more urgent the alarm, the more frequent and faster it should be.
2. Use a different sound for each type of alert wherever possible.
3. Consider if adding a verbal warning message to the alarm will be useful.
4. It should be loud enough to be easy to detect, but not be irritating.

But don't overdo it! Too many alarms can mean people ignore them at critical moments.

-
- [!\[\]\(e27c4336460e9e6729a19580c0456728_img.jpg\) Read more about Auditory alarms](#)
 - [!\[\]\(1a140e8db538fd46d58af9f9540232fd_img.jpg\) You may also want to read about Visual warnings: overview](#)
 - [!\[\]\(5a658b86f2c8900a276c586c1f8f9f2f_img.jpg\) You may also want to read about Technical integration: overview](#)
 - [!\[\]\(dde796100cc481a63a6f917e6942c754_img.jpg\) You may also want to read about Verification: overview](#)
 - [!\[\]\(63a8f188d537bd691c8d94f41db6869a_img.jpg\) Go to 3. Business as usual](#)
 - [!\[\]\(499fe69158060e68a02a9089268949e0_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(c8aba30b21c2fae4d961d3c29bf22065_img.jpg\) Go to Glossary](#)

Visitors to the control room: overview



A visitor to the control room should have a defined and clear purpose, and should be authorised by the supervisor or manager.

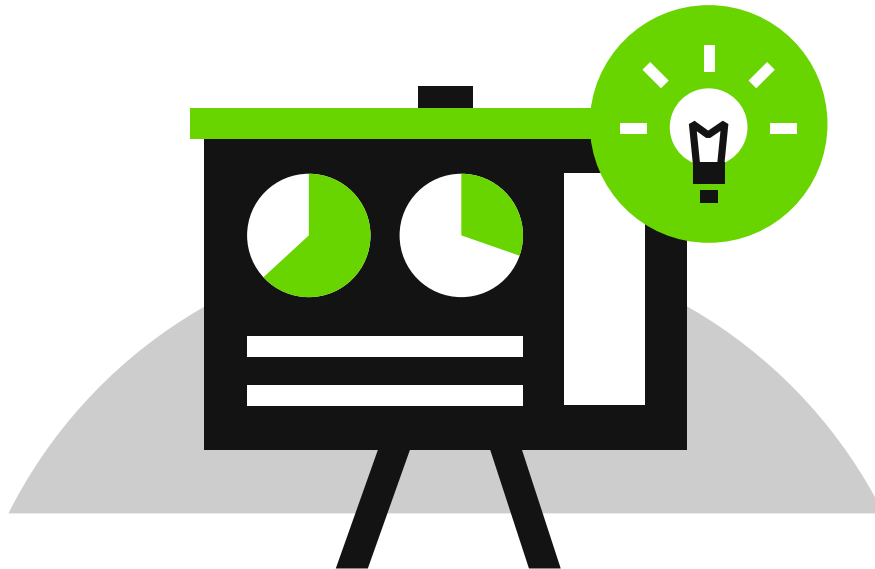
For each visitor:

1. Always sign them in AND out.
2. Check their ID before issuing a visitor's pass.
3. Appoint a named contact to meet the visitor and escort them during their visit.
4. Consider whether some parts of the control room should be obscured during their visit.
5. Monitor where they go during their visit.

If the visitor is doing sensitive work within the control room, they may need to be vetted.

-
- [i](#) Read more about [Visitors to the control room](#)
 - [i](#) You may also want to read about [Culture: overview](#)
 - [i](#) You may also want to read about [Threat: overview](#)
 - [i](#) You may also want to read about [How secure does your control room need to be?](#)
 - [i](#) You may also want to read about [Access to the control room](#)
 - [Go to 3. Business as usual](#)
 - [Go to start of \[Control Rooms Guidance\]\(#\)](#)
 - [Go to \[Glossary\]\(#\)](#)

Training: overview



Training helps people to carry out their jobs effectively. People should be trained when:

- they're new
- systems have been updated or changed
- they're returning from extended absence.

It's worth thinking about the whole picture in the control room, and training your security officers across the board, including:

- security systems
- operating procedures
- radio communications
- what to do when an alarm goes off (including false alarms)
- what to do when there's an adverse event.

i Read more about [Staff training](#)

i You may also want to read about [Response staff](#)

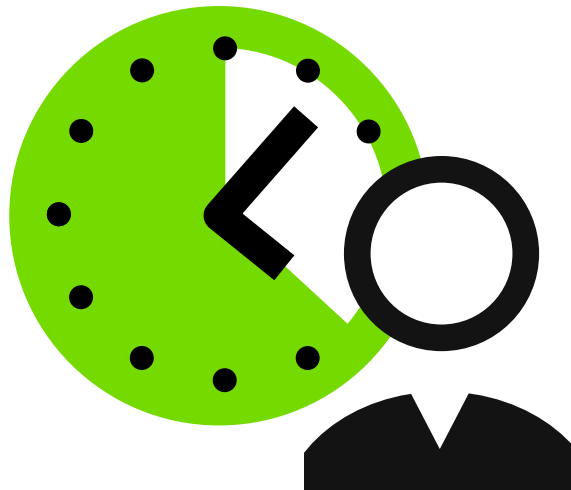
i You may also want to read about [Exercises and simulations: overview](#)

↗ Go to [3. Business as usual](#)

↗ Go to start of [Control Rooms Guidance](#)

↗ Go to [Glossary](#)

Shifts: overview









Shift work can affect people's wellbeing and performance, so supervisors should be aware of problems people might experience when they change to new shift periods.

Eight-hour shifts can mean a lower risk of errors and accidents but some people may prefer 12-hour shifts to fit their life routines. Continuous night shifts may be harmful to health.

Ideally shifts should rotate clockwise early > late > night.

Where you require a high level of vigilance of your security officers, it's best to keep tasks to a maximum of 20-30 minutes.

-
-  Read more about [Shift lengths and task rotation](#)
 -  You may also want to read about [Shift handovers](#)
 -  You may also want to read about [Staff welfare at work](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)

Recruitment: overview









People are only human. When you design a job, remember that people vary in the way they process information and share it.

It's also worth planning ahead – your team should be large enough to cover people being off sick or on holiday.

A job analysis will help you create accurate job descriptions and work out how many staff you need, and at which levels.

A structured interview is more effective than an unplanned one. It's a good idea to have the same people interview the candidates and apply ratings and checklists to assess candidates' suitability for the job.

-
-  You may also want to read about [Security officers: overview](#)
 -  You may also want to read about [Recruiting security officers](#)
 -  You may also want to read about [Staff recruitment and promotion](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Effective communications

It's vital that there's clear and effective communication between everyone – the security officers in the control room, those who are on patrol and the response team.

This is even more crucial during a security incident: it can increase the speed of response and the chances of stopping someone with hostile intent before they reach the site's critical assets.

EVERYONE ON THE TEAM NEEDS TO KNOW

1. **How to communicate** – is there a separate radio channel for incident reporting and alarm verification?
2. **Who they should talk to during an incident** – their supervisors or should they use the comms to make sure everyone on the team knows what's happening?
3. **What to do if the primary comms tools (eg radios) aren't working** – what are the backup procedures?



BACKUP PROCEDURES

If your radios aren't working you'll need to have backup procedures in place, such as a site map. Everyone in the control room and on the ground should use the same version of the map.

Your site map should show navigation points and the locations of all cameras on the site – this can help guide the response team to the location of an incident. Make sure navigation points and camera positions are logically labelled (from left to right or in a clockwise direction).

Everyone on the team (in the control room and beyond) should use the same terminology for points on the map and areas of the site. This will help avoid confusion and make it easier to give clear directions from the control room to the people on the ground.

CONSIDER WHICH TYPE OF COMMUNICATION IS BEST FOR EACH SITUATION

In a fast-moving incident, you'll almost certainly want to communicate verbally, but this may be harder to log, spoken instructions may not always be clear and details can be lost.

If you're using email, it will be important to have no delay in the message getting through. (Some sites may have an automatic 5-minute delay before emails are transmitted.) You may well need to send multimedia images or videos to the team on the ground, especially if you need to help them identify people.

If your communications include classified material or sensitive information, you'll also want to consider specifying the cyber assurance for your email system.


GOOD COMMUNICATIONS ACROSS ALL LEVELS


Your control room, incident room and operation room should be located within easy reach of each other – the teams will need to talk during an incident.


A large open space can be problematic. If noise travels, it's a good idea to have blinds or noise deadening partitions that can be used during an incident.

FURTHER READING

- **CPNI CCTV best practice guide**


 You may also want to read about [Types of guard force and control room: overview](#)


 You may also want to read about [Control room: overview](#)


 You may also want to read about [CCTV screens: overview](#)

 You may also want to read about [Windows and external lighting: overview](#)


 You may also want to read about [Resilience: overview](#)

 You may also want to read about [Technical integration: overview](#)

 You may also want to read about [User interface: overview](#)

 Go to [3. Business as usual](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Access to the control room

Visitors to the control room can distract the people who are working there and may even make the control room less secure. It's important to limit access to essential visitors only.

Your control room itself may be a target so you'll need to limit visits as far as possible.

- The control room should be electronically protected and it should require a higher level of security.
- A low throughput is fine: security – not speed – should be your top priority when checking authorisation.
- Monitor anyone who does have to visit the control room.

If you are using **biometric access**, make sure that it's easy for people to use and that it works properly. (A complex biometric access system can mean people look for workarounds to avoid using it, and that is going to be bad for the building's security.) Keep an eye on the failure rate of the system – that will help you measure its effectiveness.

KEEP A LIST OF AUTHORISED VISITORS

It's important to be clear who is allowed to add names to the list of authorised visitors. People added to the list should be authorised for a limited time.








Make sure you regularly review the list of visitors and people who are authorized to access the control room.

- Anyone no longer requiring access should be removed from the list
- Anyone requiring continued access should be asked to affirm their access requirement before authorisation is renewed.

POLICE ACCESS

You'll need a policy and process for dealing with the police when they need to access the site for any reason, such as forensics.

You'll also need to have a **specific contact or duty officer** for them to deal with. This could be a rotational duty. This will help reduce disruption for the security officers working in the control room.

-
-  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Personally identifiable information: external review](#)
 -  You may also want to read about [Visitors to the control room: overview](#)
 -  You may also want to read about [How secure does your control room need to be?](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Visitors to the control room

Visitors should have a defined and clear purpose for the visit. All visits should be authorised by the supervisor or manager.

Depending on the purpose of the visit, you may need different levels of authorisation. If the visitor is coming to see the workings of the control room, you may need supervisor authorisation. If the visitor is there to work within the control room, you may need security manager authorisation.

The visitor's credentials (organisation, vetting level and so on) may also inform you about the level of authorisation needed for the visit. If the visitor is doing sensitive work within the control room, you may need to get vetting information from their employer.

If your visitor is going to be treated as a full-time member of staff for the duration of their time with you, you may want to vet them independently of their employer.









BEFORE YOUR VISITOR ARRIVES

Before the visit begins, consider the assets that might be on view. Are they sensitive? Is the visitor OK to see all the functions/equipment/areas of the control room? You may need to screen some areas or equipment off to avoid the visitor seeing them.

You'll also need to consider the safety of the visitor and make any preparations necessary.

Here's a quick checklist:

- ✔ Always sign the visitor in AND out.
- ✔ Check their ID before issuing a visitor's pass.
- ✔ Appoint a named contact to meet the visitor and escort them during their visit.
- ✔ Monitor where they go during their visit. Use access control methods such as passes to monitor where the visitor goes.

-
-  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Culture: overview](#)
 -  You may also want to read about [How secure does your control room need to be?](#)
 -  You may also want to read about [Location of your control room](#)
 -  You may also want to read about [Access to the control room](#)
 -  Go to [3. Business as usual](#)
 -  Read the full [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Recruiting security officers

When you're considering candidates for the job of security officer, it's important to have a rigorous and thorough selection process.

In a structured interview, each applicant is asked identical questions. You can then score their answers using ratings and checklists to help you make an objective decision.

Here are some points you may want to consider when recruiting team members.

Communication skills: Do they have good spoken and written communication skills? Security officers need to communicate clearly in their work, particularly when they are dealing with an emergency.

A control room works best when there are strong team relationships and that means good communication. When the control room team and the security team on the site communicate well, this can increase situation awareness.

Physical fitness: Are they physically able to cope with the demands of the job?

Shift work: Can they cope with shift work? It can have an impact on people's health and on their personal life. If they support a young family or if they are a career, you may need to take that into account.

Using technical and specialist CCTV equipment: Are they comfortable using this kit?


Coping with change in the chain of command: Are they OK with reporting to someone who isn't their usual manager or who doesn't normally hold a more senior position in the control room? This may be necessary during an incident.

As part of the selection process you may want to ask candidates to complete specific tests.


1. **Cognitive ability psychometric test** includes aptitude tests and mental ability tests, assessing numerical and verbal/non-verbal reasoning skills.
2. **Personality psychometric test** may help to indicate potential responses to tasks. If a candidate scores highly in conscientiousness, for example, they may be more determined to see tasks through to completion.
3. **Home office English language test** to comply with SIA licensing, as control room staff must be able to communicate competently in English. This test is the required level for that work.
4. **Vision tests.** Security officers need good eyesight, with glasses or contact lenses if needed. **Visual acuity** tests the clarity of vision. This can be tested wearing glasses or contact lenses if needed. (Candidates will need vision at least at 6/20 on a Snellen chart, equivalent to reading a car number plate from 20.5 metres). **Dynamic acuity** tests eyesight with the head moving up and down as if looking at a screen. **A colour vision test** is particularly important if your control room warnings are colour coded. (This test is often done using the Ishihara 38 Plates.)

FURTHER READING

- **British Psychological Society psychological testing**


 You may also want to read about [Security officers: overview](#)

 You may also want to read about [Staff recruitment and promotion](#)

 You may also want to read about [Use case: overview](#)

 Go to [3. Business as usual](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)

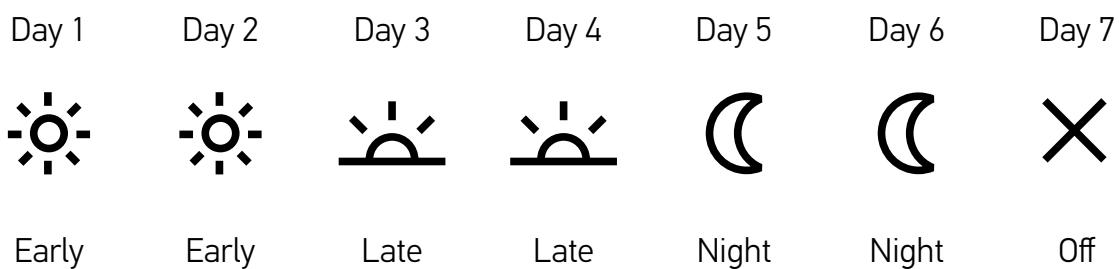


Shift lengths and task rotation

People who do shift work may find that it has a detrimental effect on their wellbeing and performance. Supervisors need to be aware of orientation difficulties for people who change to shifts to a period that they are not used to.

Ideally, people work eight-hour shifts: this can mean they experience less fatigue and stress, and they cope better with their workload. As a result you may see a decreased risk of errors and accidents. But it's not always practical to move to eight-hour shifts and some people will prefer 12-hour shifts to fit in with their other commitments.

It's best to avoid continuous night shifts (it has been linked to higher risks of heart disease).










SHIFT ROTATION

If possible, rotate people's shifts from early, to late, to night (for example a pattern might be 2 early, then 2 late, then 2 or 3 nights, followed by a 24 hour break after a night shift). This may reduce the negative effects of shift working.

TASK ROTATION

If you need to ensure people remain highly vigilant, it's a good idea to keep tasks within a shift to 20-30 minutes. Any longer risks a reduction in their level of vigilance.

-
-  You may also want to read about [Security officers: overview](#)
 -  You may also want to read about [Staff welfare at work](#)
 -  You may also want to read about [Resilience: overview](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Shift handovers

Handing over from one shift to the next is important: well done, it can make your control room more effective.

Handovers help your situational awareness: a good handover means the people coming on duty will be up to date with what's going on in the control room.

It's important to overlap shifts so that the people going off shift can hand over properly to the people starting the new shift. The time for handover should be included in people's paid shift periods.

WHAT INFORMATION SHOULD YOU SHARE DURING A SHIFT HANDOVER?




If you're a **security officer** you will probably cover information such as:

- ✓ Incidents that happened and were dealt with during the shift that is ended
- ✓ Incidents that are still ongoing
- ✓ Changes to staff / contact details
- ✓ Any technical or site issues
- ✓ Anything that is unusual or "out of the norm"
- ✓ How many security officers there are and their duty positions

If you're a **manager**, your handover briefing with the next shift manager may be different as it will include information specific to your role, such as details regarding management of staff and buildings.

USEFUL TOOLS FOR HANDOVERS

You may find it useful to include screenshots of incidents, sketch maps and bullet point summaries of what's been happening.

-
- i** You may also want to read about [Security officers: overview](#)
 - i** You may also want to read about [Effective communications](#)
 - i** You may also want to read about [Response staff](#)
 - i** You may also want to read about [Staff welfare at work](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Staff welfare at work

TAKING A BREAK

Just like everyone else, the people on your team – whether they are in the control room or on patrol – need regular breaks and access to essentials such as toilets, hand-washing facilities and drinking water.

When they take a break, people need to have a place where they can relax, chat and eat their meals, well away from anything that might contaminate their food.

SAFETY AT WORK

Where necessary, your security officers need access to appropriate personal protective equipment (PPE).

Regular breaks from computer screens will help reduce eye strain, so it's a good idea to encourage this as a good habit.


CULTURAL AND RELIGIOUS REQUIREMENTS

It's important to take account of people's cultural and religious needs, such as fasting during Ramadan, the Jewish Sabbath or bank holidays.

If the people on your team feel confident that you respect their cultural and religious needs, this can help their motivation and they are more likely to support your organisation's security more effectively.


FURTHER READING

- HSE: A brief guide to Working with Display Screen Equipment
- HSE: Welfare at Work

 You may also want to read about [Rest areas](#)

 Go to [3. Business as usual](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Staff recruitment and promotion

Here are some top tips on staff recruitment and promotion.

A job analysis will help you create accurate job descriptions

It's a good idea to create a list of jobs for each role. This will help you map organisational priorities, write person specifications, interview questionnaires and design pre-selection tests.

- Consider whether to include observation, interviews and questionnaires when recruiting staff and supervisors.

How many staff do you need, and at which levels?

Site vulnerabilities, risks and threats to your organisation are key factors when you're looking at the essential competencies your staff need.

With those defined, you can write a clear person specification describing the key competencies required for a role to carry out tasks that secure the site.

People are only human

When you're designing a job, bear in mind that people vary in the way they process information, and how they share it. How they process and share information can also affect their awareness of situations.

- It can help to think about how people absorb information, particularly when they are under stress, or have different workload levels.
- When people need to work on tasks as a team, it's a good idea to introduce clear role divisions.

A structured interview is more effective

Not all organisations have the same priorities – your analysis of the job and the person specification will be specific to your organisation.

- A structured interview has been found to be more effective one that is unplanned.
- It's a good idea to have the same people conduct the interviews throughout the selection for a role.
- Structured interviews mean you can apply ratings and checklists to all candidates so the selection process is fairer, and on their suitability for the job.

Plan ahead for staff sickness and holiday

It's important to plan ahead for times when people are ill or on holiday; your team should be large enough to cover those absences. The supervisor needs to understand the tasks covered by each role in order to manage cover during their absence.

Accreditation: a positive step towards consistent staffing

Schemes such as the Approved Contractor Scheme (ACS) exist to maintain performance standards, and ensure up-to-date training is provided in line with SIA requirements.

Raise the profile of security staff within your organisation

When your wider organisation sees your security team as an essential part of the whole organisation, it can increase your team's effectiveness.

Good relationships with all departments can give your team members a wider overview of situations and security concerns on the site. This can also help to build trust, so that people feel able to report any security concerns about their workplace.

Security matters – and so do the people who ensure your organisation's security

- Security officers' clothing should be fit for purpose – but it can also fit with the overall image of your organisation.
- By offering relevant training, you support positive career development and increase the skills base.
- If your security team is to be seen as an essential and respected part of the organisation, they need to be valued.
- This is more likely if they have a safe and healthy working environment and a clear reward structure.









People work better in a healthy working environment

The right equipment and a healthy work environment can support your security team and help them to be at their best. HSE guidelines are there to help you provide good working conditions so that your team can be most effective at work.

- It's important to support your team with the right types of display screen equipment, seating, noise levels, room temperature and light levels.

FURTHER READING

- **HSE: Welfare at Work**

-
-  You may also want to read about [Culture: overview](#)
 -  You may also want to read about [Security officers: overview](#)
 -  You may also want to read about [CCTV operation](#)
 -  You may also want to read about [Recruiting security officers](#)
 -  You may also want to read about [Staff training](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Staff training

Training is not just for new recruits. Everyone benefits from training when systems or procedures have been updated or changed, or to make sure they are up to speed when they return after a long absence.









Topics you will need to cover during training include:

- security systems
- operating procedures
- alarm response procedures.

EXERCISES

It's important to carry out security exercises regularly (at least once a year) to help you spot any gaps in your procedures and identify areas where training is needed.

Exercises help people in the control room and on the ground to experience a security incident in a safe environment, to familiarise themselves with response procedures and improve their performance as a team.

-
-  You may also want to read about [Security officers: overview](#)
 -  You may also want to read about [Exercises and simulations: overview](#)
 -  You may also want to read about [Follow-up after exercises and incidents](#)
 -  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Effective communications](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Roles and responsibilities

Here is an outline of typical roles and responsibilities in the control room. Some roles may be combined into one post. Your control room policy should offer clear guidance about which role takes priority in certain circumstances.

Security manager (SM)

- Responsible for overall security plan security
- Responsible for delivery of security provisions, long term physical measures and staffing numbers
- Liaison to the board level incident room
- Member of the incident room

Deputy security manager (DSM)

- Supports the Security manager
- Responsible for workforce deployment
- Organises operational reposting as required
- Liaison to the board level incident room
- Member of the incident room

Control room supervisor

- Manages day to day functions of the control room staff
- Deploys personnel within the control room
- Responsible for initial response to fast acting incidents
- Liaison to the incident room
- Escalates incidents to Incident rooms status
- Produces report to DSM or SM

Incident liaison officer

- To co-ordinate with the incident room when stood up
- The liaison officer will need to be separate from the control room supervisor, who will be running the control room during any incident.

Loggist

- Logs security issues as and when they arrive
- Logs alarms activations / cancellations and reasons why
- Logs decisions made
- Logs potential security issues, such as hostile reconnaissance
- Produces daily reports for control room supervisor

Communications officer










- Monitors and manages a dedicated radio channel
- Passes radio messages to the loggist
- Escalates issues to the control room supervisor

Integrated security systems officer

- Responsible for operation of the integrated security system (Intruder Detection Systems, CCTV)
- Escalates incidents to the control room supervisor
- Passes information to the loggist

Logging

- You'll need two logs – a daily log and a decision log. They can be electronic logs, but it's good to have a paper logbook in case of system failure.
- The daily log records events that have happened throughout the day, such as an attempted intruder; CCTV system down; alarm activation on PIDS zone.
- The decision log is kept for management or incident response and records the decisions taken.

-
-  You may also want to read about [Incident management](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Response staff](#)
 -  You may also want to read about [Response and decision-making criteria](#)
 -  You may also want to read about [Exercises and simulations: overview](#)
 -  You may also want to read about [Follow-up after exercises and incidents](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Map essentials

One of the control room's essential tools is the map.

Any map that you use and share with your team needs to be relevant, simple and consistent. This will help you effectively direct security officers and response teams to the location of an incident. And it will also help you direct people away from danger and towards a place of safety.

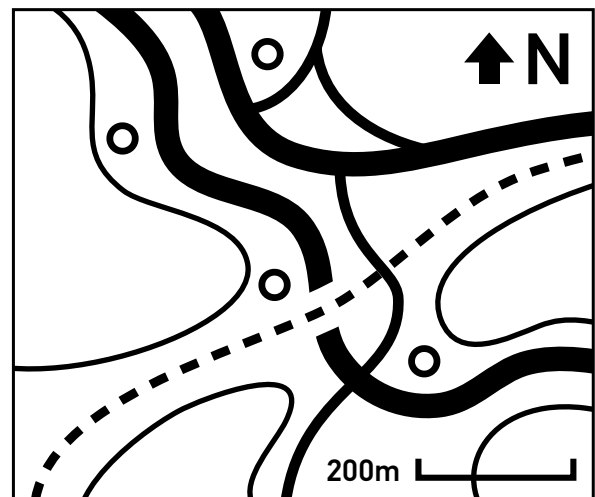
Remember to correlate your map with emergency plans, especially when you are creating an internal building map showing security features.

It's important to make sure that all the people and electronic management systems have the same map(s) – and the same view (portrait or landscape).

Top tips to bear in mind when you create maps for the control room team and security officers on the ground








1. **Keep it simple.** Make sure everything on your map is essential, and don't clutter it with anything irrelevant.
2. **Show where North is.** Conventionally it's pointing towards the top of the map.
3. **Give the map an informative title.** 'Barley Road CCTV positions' is better than 'Map 37/232'.
4. **Be consistent.** Use the same language, points of reference and search areas across all your maps.
5. **Use a legend (key)** to explain colours and symbols.
6. **Show the scale** with distances in whole numbers.

Barley Road CCTV positions



Always test a new map with users. Their feedback can help you improve the map.

If you're using a map or data from elsewhere, be sure to credit the source as maps are protected under UK copyright law.

-
-  You may also want to read about [User interface layout](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Evacuation plan: overview](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Visual warnings

A visual warning that an alarm has gone off needs to be clear, with simple text. Where it appears is important as well – it needs to catch the security guard's attention.

Here are our top tips to bear in mind when you're creating a visual warning.

1. **Keep it simple.**
2. **Use simple, clear text in a plain font** such Verdana or MS Sans Serif that is easy to read.
3. **Use symbols where you can** – symbols get the message across faster than text.
4. **Use red for the highest level of warning** (everybody knows the traffic lights colour code); green indicates safety.
5. If your warning is in black and white, make the words **TWICE** the size of warning text in colour.



For example, turning the edge of the computer screen red will alert the operator.

i You may also want to read about [Windows and external lighting: overview](#)

i You may also want to read about [Resilience: overview](#)

i You may also want to read about [Technical integration: overview](#)

i You may also want to read about [User interface: overview](#)

[Go to 3. Business as usual](#)

[Go to start of Control Rooms Guidance](#)

[Go to Glossary](#)



Auditory alarms

Alarms should cause alarm! They should be impossible to ignore.







There are often lots of false alarms in control rooms – security officers may tune out from the warning sound if they think it's probably a false alarm.

If only one type of alarm sound is used, people are more likely to miss the alarm or ignore it. So think about using different sounds and speeds for each type of alert.

Here are our top tips to bear in mind when you are creating an auditory alarm.

1. The more urgent the alarm, the more frequent and faster it should be.
2. Use a different sound for each type of alert wherever possible.
3. Consider if adding a verbal warning message to the alarm will be useful.
4. The alarm should be loud enough to be easy to detect, but not be irritating.
5. Make sure everyone knows what each alarm sound means.

And don't overdo it! Too many alarms can mean people ignore them at critical moments.

-
-  You may also want to read about [Visual warnings: overview](#)
 -  You may also want to read about [Technical integration: overview](#)
 -  You may also want to read about [Verification: overview](#)
 -  Go to [3. Business as usual](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Which type of key?

An **electro-mechanical key lock** is a mechanical key lock with added electronic control and audit function. Elements in both the key and the cylinder give assurance that the correct key is being used. If an individual key is lost, its details can be removed from the system so you don't have to replace the entire suite of locks on the site. This also means you can enable timed or one-off access for visitors.

Electronic keys are issued and programmed at a computer or programming station. Ideally this is a function for the site's pass office rather than the control room. Where the control room has to cover this function, you should make sure that issuing and programming of electronic keys is done on a dedicated computer station with access restricted to properly trained and cleared personnel. All staff dealing with electronic locks should be briefed on proper use and care of electro-mechanical keys and locks.


Lost keys are less of a problem with electro-mechanical locks – simple reprogramming can usually invalidate a lost key.


A **master key system** will help to control access at varying levels to authorised users. Typically it will comprise:

1. **Grand Master** – unlocks all doors
2. **Sub Masters** – for doors on individual floors or zones
3. **Standard** – individual room keys, each specific to one door.

FURTHER READING


- **CPNI Key control**
- **CPNI Secure destruction of sensitive items**

 You may also want to read about [Technical integration: overview](#)

 You may also want to read about [User interface: overview](#)

 Go to [3. Business as usual](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Key control

As with anything that might risk distracting security officers from their main tasks, the task of holding and issuing keys for access to the site should (in an ideal situation) be kept away from the control room.

If your answer to the next three questions is 'No', it probably makes sense to assign part or all of the key control task to the control room.

1. Do you have a pass office issuing electronic passes? They will be ideally placed to deal with the issuing and control of keys.
2. Can you site key issue and control elsewhere, such as an operations room?
3. Can access to different areas of the site be controlled by technology? If so, what security is needed for that system?

Next, consider these questions:

- Which keys need to be held within the control room?
- Does it make more sense for the control room only to deal with security-related keys? And for other operations and convenience keys to be held elsewhere?

Key control and issue is NOT just a casual responsibility, dealt with by whoever is not busy at that moment. It's best to assign the specific role of key control and issue to one post.

KEY CONTROL AND AUDIT

When a key is lost or a lock is compromised, your site's security is also at risk. Consider where each key should be held, and the asset it is protecting and level of protection it needs.

A master key system will help to control access at varying levels to authorised users. Typically it will comprise:






- **Grand Master** (unlocks all doors)
- **Sub Masters** (for doors on individual floors or zones)
- **Standard** (individual room keys, each specific to one door).

Your **key control policy** should cover each category of key (Grand Master, Sub Master, Standard), and the issuing and log requirements for each type of key.

With careful planning, you can limit the number of high security keys (and thus limit the cost) so these locks are strategically placed rather than installed on every door.

Key control and issue is a significant drain on resources in the control room

It's useful to think of the impact of key control and issue on the work of the control room team when you are designing your key control policy.

-  Key control and issue are dealt with elsewhere (not by the control room team).
-  Keys are personally issued to individual people for long periods; control room staff may have to keep a log of keys issued.
-  Keys area kept locally at each door, in a key safe (codes known to users and/or control room).
-  Control room issues security keys; less critical 'convenience keys' (e.g. to store room or cleaners' cupboard) issued elsewhere.
-  Control room issues all keys, and keys are mustered at the end of the day.

RULES FOR KEY CONTROL

If your control room is responsible for key control, there are some essential rules to observe


1. **Define your policy for control and distribution of keys and locks – and limit access to approved users.**
2. High security keys should never leave the building they protect.
3. Restrict the number of keys issued to the minimum.
4. **You should know where each key is at all times.** Unless issued, they should be kept securely (eg in a key-keeper cabinet).
5. Only release keys to an approved user.
6. Whenever a key is issued, log that event with date, time and person to whom it was issued.
7. **Instruct users never to lend keys to anyone else** and to store them out of sight.
8. You'll need a policy and process for dealing with lost keys and replacing locks. It's important to specify if spares are held on site with sufficient keys for all authorised users, or whether a supplier is on call to cover the work.
9. Locks and keys that are no longer needed should be disposed of securely.
10. Every 6-12 months, it's a good idea to **carry out a random muster of all keys** to check that each one is still with the person who signed them out.

FURTHER READING


- CPNI Key control
- CPNI Secure destruction of sensitive items


 You may also want to read about [Personally identifiable information: internal review](#)

 You may also want to read about [Personally identifiable information: external review](#)

 You may also want to read about [Monitoring the control room](#)


 You may also want to read about [Incident response plan: overview](#)

 You may also want to read about [Exercises and simulations: overview](#)

 You may also want to read about [Staff training](#)

 Go to [3. Business as usual](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Other control room functions

Time away from CCTV monitors is essential for all security officers: too long staring at CCTV screens can lead to fatigue, loss of concentration and even boredom.

SHADOWING COLLEAGUES

When you shadow colleagues it can help everyone involved: you can form good working relationships and gain a broader understanding of roles and procedures.

Shadowing colleagues on the ground can improve communication between the teams. Walking the plot with the security officers who patrol there every day can help you understand how each camera view relates to the real ground. Whether you're in the control room or on the ground, it helps to know the position of each camera and this can then improve communication between teams during incidents.

OTHER COMPUTER TASKS

There will also be other work-related tasks that everyone in the control room will need to do, such as completing timesheets and answering emails. These are best done at non-CCTV computers to avoid distracting colleagues.

DISTRACTIONS

If security officers are also required to carry out non-related administrative or reception tasks, these should be done away from the main control room to avoid distracting the rest of the control room. These tasks could include:

- attending car parks
- answering phones
- receiving personal deliveries.
- managing lost property
- managing reception

It's worth considering whether these tasks are a good use of security officers' time: you may find it is more cost-effective to employ an administrative person to cover them.

i You may also want to read about [Types of guard force and control room: overview](#)

i You may also want to read about [Control room: overview](#)

i You may also want to read about [CCTV screens: overview](#)

i You may also want to read about [Windows and external lighting: overview](#)


i You may also want to read about [Resilience: overview](#)

i You may also want to read about [Technical integration: overview](#)

i You may also want to read about [User interface: overview](#)

 Go to [3. Business as usual](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)

Incident response plan: overview

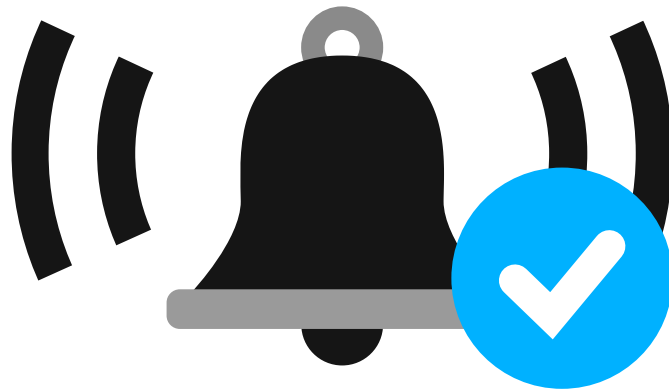


An incident response plan should include:

1. Information specific to the site
2. Escalation procedures
3. Who is in overall control and makes decisions
4. Who responds to an incident
5. Where to move to during an emergency
6. Evacuation procedures.

-
- [i](#) Read more about [Incident response plan](#)
 - [i](#) You may also want to read about [Incident management](#)
 - [i](#) You may also want to read about [Response and decision-making criteria](#)
 - [i](#) You may also want to read about [Response: overview](#)
 - [i](#) You may also want to read about [Evacuation plan: overview](#)
 - [Go to 4. Incident response](#)
 - [Go to start of Control Rooms Guidance](#)
 - [Go to Glossary](#)

Verification: overview



In some cases, when an alarm is triggered an automated, low level response can be deployed automatically.

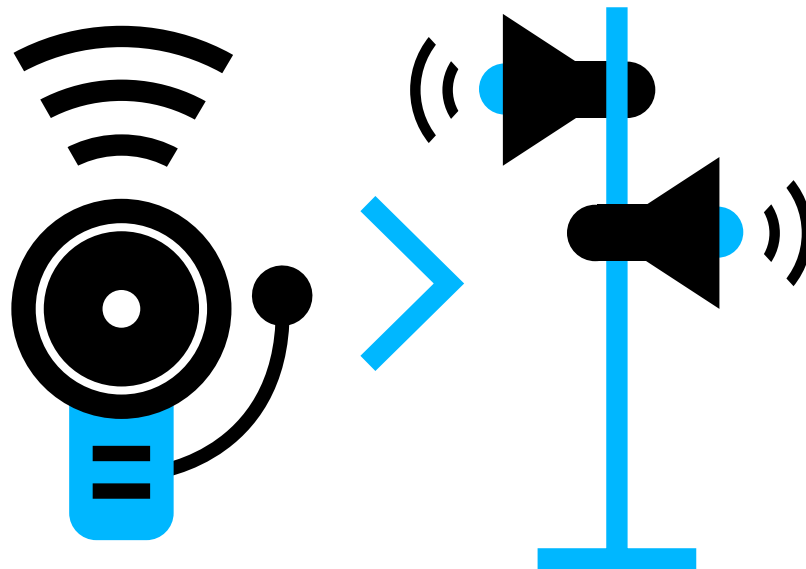
Verification may be done:

- **by CCTV** – this is the most common way to confirm a perimeter or automated alarm.
- **by a human** – a security officer on the scene can give a richer picture; they can interact with the scene, ask questions and interpret behaviour.
- **All alarms should be verified** as either a false alarm or a real alarm.

Be aware that repeated false alarms may be ignored – and could lead to people ignoring the alarm that is triggered by an event.

-
- [i](#) Read more about [Verification](#)
 - [i](#) You may also want to read about [Incident response plan: overview](#)
 - [i](#) You may also want to read about [Escalation: overview](#)
 - [i](#) You may also want to read about [Response: overview](#)
 - [i](#) You may also want to read about [Evacuation plan: overview](#)
 - [🔗](#) Go to [4. Incident response](#)
 - [🔗](#) Go to start of [Control Rooms Guidance](#)
 - [🔗](#) Go to [Glossary](#)

Escalation: overview



Escalations procedures should be written with clear, consistent language. Incident levels should be useful words that are clear to people without specialist knowledge – High, Medium, Low and Information.

An incident management checklist should be available.

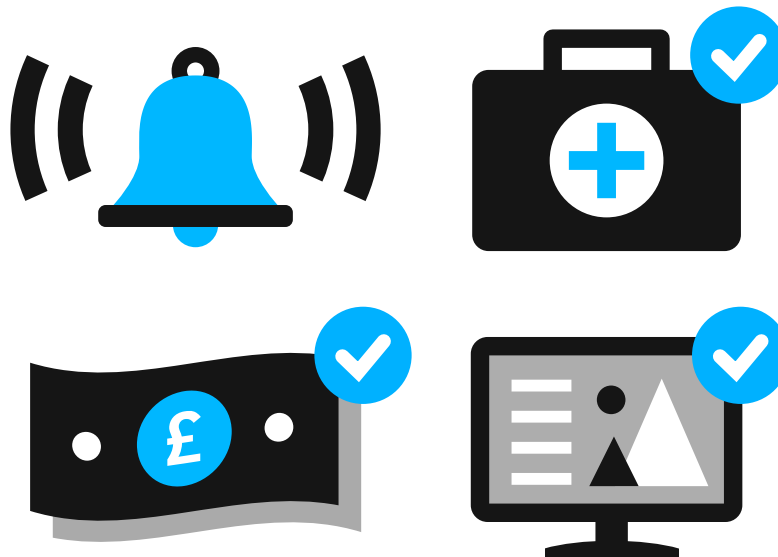
Structures and reporting lines should be clear. These may differ for day and night shifts. Reporting lines may be different for varied events.

Security officers should be encouraged to report incidents – they have the responsibility and autonomy to report issues.

Short reporting lines minimise the likelihood of information being altered between the incident and the top of the reporting line.

-
- [!\[\]\(c33cb967c8fc4f5e27188a389b621c8e_img.jpg\) Read more about Escalation](#)
 - [!\[\]\(38e1383487ca0f0e9e2c9378b9dbcae7_img.jpg\) You may also want to read about Incident response plan: overview](#)
 - [!\[\]\(d399648641177ccf0f777d76c74f84ed_img.jpg\) You may also want to read about Verification: overview](#)
 - [!\[\]\(d32727c446c8638ae1599c3d4f46ad10_img.jpg\) You may also want to read about Response: overview](#)
 - [!\[\]\(af3a820412cab4640f1b0ff6288cd856_img.jpg\) You may also want to read about Evacuation plan: overview](#)
 - [!\[\]\(12f929b5ec67e02f5e65eeeaf3df99e5_img.jpg\) Go to 4. Incident response](#)
 - [!\[\]\(7386c1d06e937b48b25a2240ff896668_img.jpg\) Go to start of Control Rooms Guidance](#)
 - [!\[\]\(ac216e2966b1433b81d3f743e456c9f6_img.jpg\) Go to Glossary](#)

Response: overview












The response to an incident should be proportionate and necessary.

If you need to bring in other agencies, you'll want to take account of each agency's powers, policies and limitations.

You should log actions, hazards and decisions. This may be useful for the lessons learnt and evidence.

Be consistent when you decide what takes priority – saving lives will usually be at the top of the list.

-
-  You may also want to read about [Response and decision-making criteria](#)
 -  You may also want to read about [Response staff](#)
 -  You may also want to read about [Incident management](#)
 -  You may also want to read about [Evacuation and critical staff](#)
 -  You may also want to read about [Surrendering to and retaking from other agencies](#)
 -  You may also want to read about [Evacuation plan: overview](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)

Evacuation plan: overview



Each site should have an evacuation plan that covers:

- 1. a full site evacuation** – all staff evacuate to the nearest exit, or are directed to exits away from an area that is currently dangerous
- 2. an evacuation based on role or criticality of job**, determined by the control room.

Each evacuation plan should include a simple map on the wall with information about exit throughputs. This helps the control room to manage an evacuation.

Different incidents may require different evacuation orders.

If staff need to be evacuated based on role or criticality of job, their roles and posts will need to be assessed first and mapped against a specific set of incidents.

-
- [i](#) You may also want to read about [Incident response plan: overview](#)
 - [i](#) You may also want to read about [Response and decision-making criteria](#)
 - [i](#) You may also want to read about [Response staff](#)
 - [i](#) You may also want to read about [Evacuation and critical staff](#)
 - [i](#) You may also want to read about [Surrendering to and retaking from other agencies](#)
 - [Go to 4. Incident response](#)
 - [Go to start of Control Rooms Guidance](#)
 - [Go to Glossary](#)

Debriefs: overview



Every person involved (at each level) should be debriefed after an incident or an exercise. If someone involved has been negatively affected, you may need to offer support.

Managers should consider any lessons learnt and update plans accordingly to improve future responses.

Hot debriefs take place within an hour of the incident. You should try to:

- establish 'Who, What, Where?' while information is still fresh in people's memory
- record the facts (though different people's views of the facts may conflict)
- note opinions about the incident.

Cold debriefs occur once the incident is over. Generally, they:

- collate details or evidence that may inform the final report
- provide conflicting accounts as people begin to forget details and maybe fill in gaps.

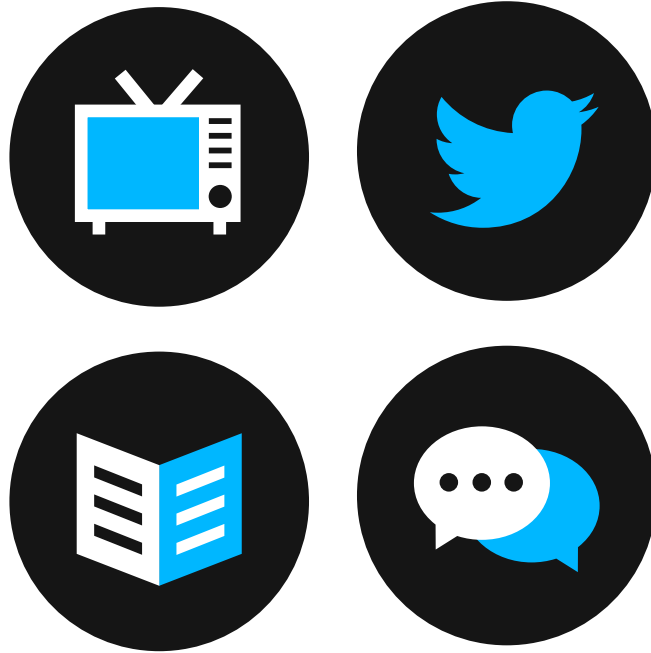
[!\[\]\(cf531ed27e91483460120fcc057b3901_img.jpg\) Read more about Post-incident debriefs](#)

[!\[\]\(d3102649f02e825ddb76dc3de0190154_img.jpg\) Go to 4. Incident response](#)

[!\[\]\(4b7a79268f6ba26c1471d4232fffa85a_img.jpg\) Go to start of Control Rooms Guidance](#)

[!\[\]\(95b425611cbd2b8716a140cf67c81822_img.jpg\) Go to Glossary](#)

Media and outside communications: overview









A good relationship with the media is useful: the media knows they are welcome to receive information, but understand their responsibilities.

If you provide **a dedicated area of the site for members of the media** to witness events, it can help the control room to monitor their access and keep people safe.

When you keep local residents informed about an incident, it can help build trust. If local people know you will update them, it may mean that fewer people will come to the site for more information.

Mass messaging (such as a phone line with a prepared message) may be useful in this situation.

-
-  You may also want to read about [Incident management](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Escalation: overview](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)












Incident response plan

When developing a security plan, sites will need to take into account the culture and risk appetite of the organisation, and any organisation-wide security policy decisions. Individual sites will then need a site specific plan, detailing where to move to during an emergency, site specific evacuation procedures etc.

There should be a clear understanding of who is in overall control during an incident. All staff should know who has the authority to make decisions. This may change between business-as-usual and an incident, but the change of authority should be clearly communicated.

Your site policy for the incident room should define how long an incident can run for before it is escalated. For example:

Duration	Measures
Up to 1 hour	Managed by on duty staff
1 – 4 hours	<ul style="list-style-type: none">Escalated to ongoing incident; additional functions dropped to increase staffing levelsAdmin staff allowance, refreshments providedNotify the team that they may have to work additional hours
4 – 8 hours	<ul style="list-style-type: none">Additional staff bought inNotify families that staff may be delayed due to the ongoing incident
8 – 24 hours	<ul style="list-style-type: none">Extra facilities staff brought in, for example kitchen staff to provide more meals
Over 24 hours (if threat dealt with)	<ul style="list-style-type: none">Incident now a long term issue – moves to rebuild / re-secure projectIncident room stood downControl passed to facilities team

-
-  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Response: overview](#)
 -  You may also want to read about [Verification: overview](#)
 -  You may also want to read about [Escalation: overview](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Roles and responsibilities](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Incident management

When an incident occurs, it may be necessary to inform staff both on and off site. Those remaining on site will need to know:

- What their role is
- The role of any external teams called to the site

Always keep acronyms and site-specific jargon to a minimum. This helps keep communication between both internal and external parties clear.

INFORMING STAFF AND FAMILIES

Inform staff about the incident and what they should do (if anything). If the incident occurs out of business hours, it helps if you have a pre-planned communication route, for example each manager is responsible for contacting their team.

Remember these three key points:

1. Keep information clear and concise.
2. Inform staff on other sites.
3. Update staff when necessary.









INFORMING THE MEDIA

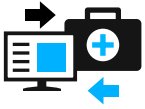
A good relationship with the media is beneficial: they know that they will be kept updated with **relevant, timely information**, but with an understanding of their responsibilities during an ongoing incident. Having a dedicated area of the site where the media can witness events can also help you to control access.

INFORMING LOCAL RESIDENTS AND STAKEHOLDERS

Informing local residents and stakeholders about an incident helps maintain a good relationship and generates trust: they will know that an incident is being dealt with, and what action, if any, they need to take. If people trust that you'll keep them informed, this may mean fewer people contacting or coming to the site directly to find out what's going on.

You can pre-plan this kind of mass communication with these groups by simple means such as a phone line with a prepared message, or bulk text messaging.

-
-  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Response staff](#)
 -  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Effective communications](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Response and decision-making criteria

The response to an incident or operation should be proportionate and necessary. When you are working to develop an incident response strategy, the partners involved should consider the policies, responsibilities and powers that are available to help resolve it successfully.

Where a multi-agency response is required, check if partner agencies have any specific powers, and policies that they are required to follow. You may find that your partner agencies have greater (or more limited) powers to undertake a specific role in the response.

HEALTH AND SAFETY

All partnership agencies have a duty in law to comply with the Health and Safety at Work Act 1974, and other relevant statutory provisions and recognised codes of practice to provide, as far as is reasonably practicable, a safe working environment.

- Those in command are responsible for ensuring that health and safety risk assessments have been completed for all tasks, and that safe systems of work are in place and communicated to all staff.
- Managers should understand and be able to supervise the health and safety risk assessment process.
- During an incident, an on-the-spot assessment of the hazards should be undertaken and noted in a risk assessment document to provide an audit trail. (Note that this on-the-spot risk assessment is not a substitute for a formal risk assessment for all anticipated scenarios.) All risk assessments should be regularly reviewed.
- The person recording the assessment should record any health and safety decisions made during an incident.

DECISION-MAKING CRITERIA

Sometimes during an incident a choice has to be made between two competing sets of priorities.











To take these decisions swiftly and effectively, you need to apply **a consistent set of criteria** to help you to prioritise correctly.



PRIORITIES TO CONSIDER WHEN MAKING DECISIONS

It's a good idea to assign priorities in accordance with a basic hierarchy like this:

1. **Personal safety** – threat to life and possible medical issues or consequences
2. **Event success** – issues that could affect the outcome (operational success) of an event, including how the community would respond to the event
3. **Media impact** – issues that could have high media and broadcast visibility or significant impact on the your organisation's reputation
4. **Financial** – issues that could have a significant financial impact
5. **Clients** – issues that affect your organisation's relationships with client groups.

-
-  You may also want to read about [Types of guard force and control room: overview](#)
 -  You may also want to read about [Control room: overview](#)
 -  You may also want to read about [CCTV screens: overview](#)
 -  You may also want to read about [Windows and external lighting: overview](#)
 -  You may also want to read about [Resilience: overview](#)
 -  You may also want to read about [Technical integration: overview](#)
 -  You may also want to read about [User interface: overview](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Verification

When an alarm is triggered, an automated low level response can be deployed in some situations. If an alarm needs a more committed or costly response then it needs to be verified.

All alarms should be verified and recorded, whether they are real or false alarms.

Verification by CCTV is the most common way to check what triggered a perimeter or automated alarm.

When the alarm is triggered, the CCTV display will automatically show the related view. For this to work properly:

1. CCTV and alarm systems must be accurately linked or cross-referenced.
2. CCTV picture quality needs to be fit for purpose. (Do you need to spot someone on the scene, or do you need to see what is happening in more detail?)
3. Lighting or infra-red illumination should be in place to give the required visibility.
4. Pre-event footage, if needed, must be good enough quality (resolution and frame rate) for security officers to understand what is happening.

Verification by thermal imager will probably show not enough detail to help resolve an alarm, as details in the picture are lost and it is harder to interpret. Most views of a fence line will look very similar, especially at night, so it's important to display CCTV camera numbers and PIDS zones on the screen.

Verification by a human can give a richer picture than verification by CCTV. People can interact with the scene, ask questions and interpret behaviour when they are on the spot. If there is no CCTV coverage of the area or interest, or if more information is needed, a security officer may be deployed to verify an alarm. Before you send a security officer to an alarm notification, consider if it's safe to do so, particularly if it looks like it may be a site attack.

When someone reports an incident directly to the control room, this information should be recorded and assessed immediately then, if credible, followed up with verification by CCTV or a security officer.

REPEATED FALSE ALARMS

If there are repeated false alarms, people can be lulled into a false sense of complacency. So the causes of regular false alarm should be investigated. Often it will be due to an incorrectly installed or configured system or an inappropriate use of technology. Make sure these problems are dealt with as soon as possible.

FALSE ALARM RATE

The number of false alarms you are likely to experience will vary. One factor is the length of your site's perimeter and the proportion of security guards on patrol per km of perimeter.

If there are too many false alarms, the people monitoring the system will be unable to cope – they may simply ignore an alert, or silence the alarm but not investigate it, or find ways to inhibit the alarm.

Generally, between 5 – 10 false alarms per day / per km of perimeter monitored by the detection system is acceptable and achievable without overloading the people monitoring CCTV screens.

DEALING WITH FALSE ALARMS

You may need to consider inhibiting an alarm during working hours (for example a door contact) or the retuning the system to allow for local conditions. Sometimes during bad weather, false alarms are excessively high and it is acceptable to inhibit an alarm – but this should happen no more than 5 times (24 hour period) a year. If your system is false alarming more than these values, check the installation or consider changing it.








- If an alarm is verified as a false alarm, this should be logged and details of the cause noted.
- **Don't ignore repeat false alarms: escalate and investigate.**

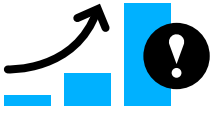
DEALING WITH TRUE ALARMS

With true alarms, what happens next will depend on the type of incident.

If the incident is static, for example a VBIED (vehicle-borne improvised explosive device), verification will be a simple task. The control room can then pass the management of the incident to the Incident room, allowing the control room to focus on their work.

If the incident is a complex or a fast-moving attack, the control room may well need to deal with the immediate response rather than escalate it to the incident room.

-
-  You may also want to read about [Visual warnings: overview](#)
 -  You may also want to read about [CCTV operation](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Escalation: overview](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Escalation

It's important to define levels of incident and clear procedures for escalation.

- Escalation procedures should be written with clear, non-specialist language that is clear to everyone.
- Incident levels can usefully be defined in everyday terms: High, Medium, Low and Information.
- Security officers have a 'crib sheet' version for quick reference.

A SAMPLE ESCALATION PLAN

Level	!!! High	!! Medium
Definition	<p>CRISIS</p> <ul style="list-style-type: none"> • A situation that results / may result in: serious harm to people, substantial damage to property or significant disruption to operations; • OR: a situation that has occurred / is ongoing, that could have a major negative impact 	<p>INCIDENT</p> <p>A situation which has occurred or is ongoing that could have a negative impact on operations</p>
What is happening	<ul style="list-style-type: none"> • Your site has stopped operating or is severely impacted • Many/all client groups impacted (including general public/local community) • All functions affected • Major media coverage 	<ul style="list-style-type: none"> • Your site's operations are impacted; possible consequences to other operations / events • Significant number of client groups impacted (including general public/local community) • Affects a significant number of functions/sites • Significant media coverage
Control room response	Immediate escalation to Incident Room	Immediate escalation to Incident Room
Incident room response	Immediate escalation to Board level + Incident room set up + Operational management of incident	Briefing to Board level + Incident room set up + Operational management of incident + Strategic management of incident
Board level response	Strategic management of incident	

Level	! Low	i Info
Definition	ISSUE <ul style="list-style-type: none"> An event that may trigger or escalate an incident or crisis 	FOR INFORMATION ONLY No action required
What is happening	<ul style="list-style-type: none"> Operations delayed but no consequences to other operations / events Small number of client groups impacted Affects a small number of functions or venues Little media coverage 	<ul style="list-style-type: none"> Change to normal operations but with simple workaround Solved on the spot Affects a single client, function or venue Not visible to the media
Control room response	Include in daily report	Include in daily report for trend analysis
Incident room response	Perform trend analysis + Ensure issue is resolved + Where necessary, provide resources to resolve issue	Perform trend analysis
Board level response		

KNOW WHO YOU REPORT TO WHEN THERE'S AN INCIDENT

It's essential that everyone knows who they report to in the event of an incident. If there are different reporting and escalation structures for daytime and night-time, this should be clearly identified. And make it clear what times when these become effective (for example, you may need to spell out whether 17.30 comes under the day or night structure).

INCIDENT MANAGEMENT CHECKLIST

There should be a generic issue / incident checklist available as a reference tool for the security and management team. This provides a framework for issue resolution and escalation, and should include:

1. Potential need to escalate for information or action
2. Impacts for liaison officers in the Control Room
3. Impacts for other sites
4. Impacts on any other partners
5. Corporate impacts
6. Reputation impacts in the media
7. The need for further analysis
8. The need to share information with delivery partners

A CLEAR ORGANISATIONAL CHART












It's important to have a clear organisational chart available: this helps with the escalation and management of incidents. It should detail all security stakeholders (in the security team and beyond) and how they relate to each other.

Stakeholders outside the security department may include the operations department, facilities management, senior board, external agencies, regulators, media outputs, intelligence inputs and so on.

ALL STAFF NEED TO BE CLEAR ABOUT THE PROCEDURES FOR ESCALATING INCIDENTS

Here are some key points to bear in mind when planning how to escalate an incident:

- **A clear reporting process** identifies what is required of each member of the team during an incident.
- **Short reporting chains** reduce the risk of information being lost or altered between the original report and the top of the reporting line.
- **Depending on the type of incident, you may need different reporting lines.** Sometimes you may find that advice on handling the event comes from a colleague, not a manager.
- Security officers can be encouraged to report issues and incidents by reminding them that they have both the responsibility and the authority to do so.
- Some events don't need to be escalated as they can be managed by on-site supervisors. However, it needs to be clear what types of event fall into this category, and the list reviewed regularly.

-
-  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Incident management](#)
 -  You may also want to read about [Verification: overview](#)
 -  You may also want to read about [Response staff](#)
 -  You may also want to read about [Evacuation and critical staff](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Response staff

The response to an incident may require staff levels over and above business-as-usual operations. You should prepare for this increase in incident planning.

Roles that may need a surge in staff should be identified in advance. As well as security officers you may need to plan for:

1. Managers (security officers will be less effective if their managers are tired)
2. Admin staff
3. Facilities management
4. Catering staff

Other departments will need to understand what will be required of their team during an incident, so they can plan accordingly.











- IT support and maintenance may need additional staff or longer hours to support the control room during an incident
- While facilities management may not need additional staff, they may require a call out function in order to prepare and support an incident room.
- While 24 hour catering may not be practical, catering staff may need to work later to provide an evening meal, for example. Where an incident runs through the night, you may need to nominate someone to bring food and drink to the incident room to maintain staff performance levels.

During an incident, normal rotation of staff will probably be halted and those who are in post at the start of the incident will remain in position. It's worth bearing in mind that:

- During periods of heightened alert staff can maintain focus longer than during business and usual activity.
- If the same people remain in position, situational awareness will be higher.
- You may need fewer staff in total if rotation is not taking place (as there are no staff 'between posts'). This can free people to man an incident room.

If it can be done securely, it can be a good idea to have incident room members join the discussion by tele/video conference. This may be particularly useful at board and strategic level, or at the beginning of an incident. It can allow decisions to be made and implemented much more quickly than waiting for people to reach the incident room in person.

It may be useful to have jackets or tabards (with names on the back or front, or name badges) so that everyone is easily identifiable in the incident management room. This is particularly important in a large organisation where people may not know each other or when you are working with outside agencies.

-
-  You may also want to read about [Network function](#)
 -  You may also want to read about [Resilience: overview](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Shift lengths and task rotation](#)
 -  You may also want to read about [Evacuation and critical staff](#)
 -  You may also want to read about [Incident response plan](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Evacuation and critical staff

FULL EVACUATION

If a full site evacuation is ordered, you may want to declare an 'evacuate to the nearest exit' order, or to have the control room manage the evacuation.

1. **Staff are directed to a specific exit or away from an unusable exit.**

This approach should be used if a specific section of a site is currently dangerous or a given route would lead to staff becoming trapped. You need to have assessed routes and exits in advance for this type of evacuation, so that you know how many staff can use an exit safely in a given timeframe, and the number and distribution of staff across the site.

To manage this kind of evacuation, the control room needs a simple map on the wall with information about exit throughputs. This will enable them to decide which exits to open and which to keep closed to maintain a secure perimeter.

2. **Staff are evacuated based on criticality of role.** To enable this, roles should be assessed and mapped against a set of potential incidents, as different incident types may require different evacuation orders. For example:

EVACUATION ORDER









Incident: Protestors intent on damage

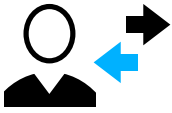
- | | |
|---|----------------------|
| 1. Cleaning and facilities management staff | 3. Operations staff |
| 2. Admin staff | 4. Maintenance staff |
| | 5. Security staff |

STAGED EVACUATION

A staged evacuation allows the minimum number of people to be evacuated for a given incident, and allows the fastest possible return to normal operations after an event.

Bear in mind that some staff may need to 'lock and leave' (prepare for evacuation and then leave) rather than leave immediately.

-
-  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Response and decision-making criteria](#)
 -  You may also want to read about [Escalation: overview](#)
 -  You may also want to read about [Surrendering to and retaking from other agencies](#)
 -  You may also want to read about [Incident management](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Surrendering to and retaking from other agencies

To manage some events you may need the support of other agencies.

You'll need to decide what will be taken over (for example, control of an ongoing incident) **and what will not be taken over** such as safety functions of the plant.










All staff, regardless of their reporting lines, have a duty to report and escalate incidents: the route for that escalation may vary depending on the situation (an active shooter would demand rapid escalation; a protest incident might at first be managed by the existing control room).

Here are some points to bear in mind.

KEEP COMMUNICATION AND ROLES CLEAR

1. **Create a clear procedure for surrendering control to external partners.** And practise using it during exercises.
2. **Agree on common terminology to aid communication across agencies.**
3. **Provide clear briefings to the new agencies.** Appoint an individual from the site to do this.
4. **Ensure that there is a formal handover of control to the new agency** and that roles of all staff are clear. (Everyone needs to understand that their original roles may change when external agencies are on site.)
5. **Log issues as they arise**, so that they can be avoided during future incidents.

When the incident is over and you retake control from external parties, they should similarly give you a clear briefing and formally hand over the control to your team.

-
-  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Shift lengths and task rotation](#)
 -  You may also want to read about [Personally identifiable information: external review](#)
 -  You may also want to read about [Response staff](#)
 -  You may also want to read about [Incident management](#)
 -  You may also want to read about [Evacuation and critical staff](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Post-incident debriefs

A post-incident debrief is an opportunity to reflect on and learn from an incident, so that everyone can improve responses in the future.

Hot debriefs review the response immediately after the event, while **cold debriefs** take place a little after the event, allowing time to collate any further information required for inclusion in a final report.

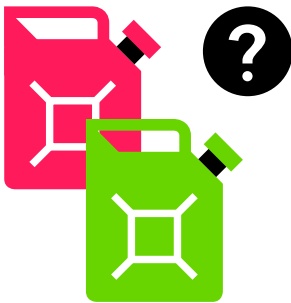
The sooner a debrief occurs, the more likely it is that witnesses will remember the facts as they happened.

People lose a lot of detail about what they witnessed within 20 minutes of an event being witnessed, and this process continues over time.

So it is logical that people can often recall considerably more detail is likely they are asked to describe what happened as soon as possible after an incident occurs.

Keep witnesses separate. When people start to discuss incidents in a group, facts can become blurred as each individual's own memories converge towards a consensus view of what happened.

The human mind tends to unconsciously "fill in the gaps" when questioned if there is no clear memory of the details. Witnesses may inadvertently create memories so that what happened makes sense to them.



GREEN OR RED? A TRUE STORY

People witnessed an individual fleeing from the scene of a crime at night time holding a petrol can. The witnesses saw this under high pressure sodium lighting.

When questioned, some of the witnesses (primarily those over 45) reported that the petrol can was red. Others, mainly those under 45, said it was green.

In fact, under this type of lighting, the can would not present a definite colour, so the witnesses unconsciously filled in the gaps from their memory.

The older witnesses 'knew' the can was red because when they were growing up petrol cans were always red. The younger witnesses assumed the can was green because that has been the standard colour for petrol cans since unleaded petrol became the norm.

HOT DEBRIEFS

These are the main things to bear in mind for hot debriefs. They should:

1. Take place within an hour of the incident.
2. Establish what occurred and where it happened.
3. Be factual as opposed to being based on individual opinion.

It's important to ensure that anyone involved is not negatively affected. If staff have been distressed, it may be necessary to offer support. This may include sending staff home. In that case, you may need to draw on extra staff as laid out by any existing contingency plans regarding staff illness or absence.










It may be useful to make a template for use in a hot debrief. This can help the witness to provide answers to the main Who?/What?/Where? questions about the incident while the information is still fresh in their memory. It's also a good way to ensure that all staff are asked for the same basic information.

COLD DEBRIEFS

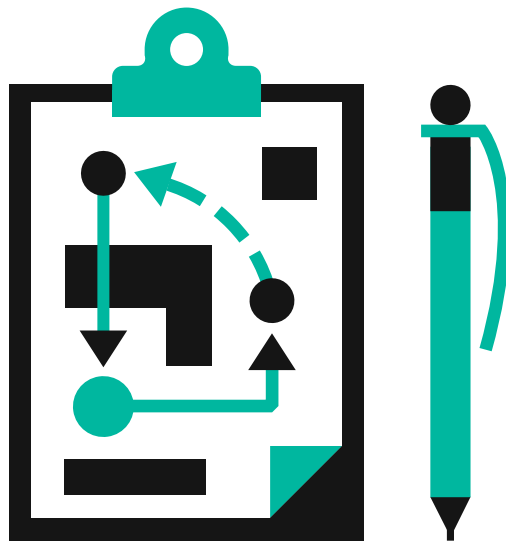
Cold debriefs happen after the incident is over. They allow you to collate any further details or evidence that may support the final report.

Bear in mind that cold debriefs may provide conflicting accounts. Managers will need to be aware that:

- There are likely to be differences in people's accounts and variations from the reports provided at the time of hot debrief.
- These differing accounts are those individuals' perceived memories (not intentionally wrong information) as witnesses begin to forget details and 'fill in' gaps.

-
-  You may also want to read about [Training: overview](#)
 -  You may also want to read about [Exercises and simulations: overview](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Staff welfare at work](#)
 -  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Follow-up after exercises and incidents](#)
 -  Go to [4. Incident response](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)

Exercises and simulations: overview














Exercises and simulations help your team to understand what is suspicious and how to respond.

It's a good idea to practise typical scenarios faced by the organisation. An exercise should:

- include control room staff, ground force and external agencies where possible
- incorporate elements such as communications, handover and escalation
- reflect real incidents
- include test scenarios where the unexpected can occur.

Table top exercises help staff practise scenarios within a secure environment and can improve performance during a real incident.

-
-  Read more about [Exercises and simulations](#)
 -  You may also want to read about [Planning exercises](#)
 -  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Staff training](#)
 -  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Resilience: overview](#)
 -  Go to [5. Exercising](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Planning exercises

When you're planning exercises – and when you're carrying them out – it's important to remember that the site still has to function normally.

KEEP WATCH FOR REAL INCIDENTS

While some of your team are carrying out exercises, you still need security officers to maintain vigilance in case a real incident happens. Make sure everyone knows how any incident should be managed.

Spell out your expectations. Be clear when the exercise is starting. Be specific about whether you are testing the response, or whether you are starting from a point where the response has already occurred.

PLAN YOUR STAFFING REQUIREMENTS

You'll need more people on shift so that the site's day-to-day running is not affected while people are carrying out the exercise.

You may need to plan for additional contingency staff to cover for people who need time off after completing the exercise.

If some people offer to carry on working after they finish the exercise, consider whether this is a good idea. Will they be too tired, less alert? How will it affect their shift pattern?











As you plan your exercise, bear these points in mind:

1. **Staff welfare is important** so make sure that everyone has access to refreshments and toilet breaks during the exercise.
2. **Do you need more room?** You may need more space to cover the admin and direct the exercise.
3. It's useful to **log the exercise** to inform forward planning and technical maintenance requirements.
4. **Be aware of other exercises.** There may be other exercises such as fire drills planned.

MEDIA AND VISITORS

You may want to give advance warning to local businesses and the media about exercises, and to brief them during real incidents.

If appropriate, consider having a clearly designated area where media and VIPs and authorised visitors can watch the incident as it unfolds. This area should be situated away from the working areas to avoid distracting people from their work on the site and in the control room.

-
-  You may also want to read about [Use case: overview](#)
 -  You may also want to read about [Threat: overview](#)
 -  You may also want to read about [Staff training](#)
 -  You may also want to read about [Roles and responsibilities](#)
 -  You may also want to read about [Effective communications](#)
 -  You may also want to read about [Incident response plan: overview](#)
 -  You may also want to read about [Resilience: overview](#)
 -  Go to [5. Exercising](#)
 -  Go to start of [Control Rooms Guidance](#)
 -  Go to [Glossary](#)



Exercises and simulations

Exercises and simulations of different potential events are an important part of continuing professional development.

They help your team develop a consistent approach to situations, to understand what is suspicious within a particular environment, and to familiarise themselves with different working structures.

By **exercising typical scenarios**, you can test work practices, procedures and individual roles within each incident.

Training should cover each role's part in:

1. Communications
2. Logging
3. Escalation
4. Handover
5. Operating procedures
6. Security systems
7. Alarm response procedures

WHO TAKES PART?

You'll need to include security officers who work in the control room and on the ground, as well as external agencies (where possible).

WHAT SHOULD YOU COVER?

- At guard level, e.g. training in specific technology
- At individual technology / machine level, for example testing alarms
- At systems level, eg penetration testing

Remember to test fall back systems as well as the main system.

WHERE SHOULD YOU CARRY OUT EXERCISES?

It's important to carry out training on site so that it reflects real incidents in the place that your team is responsible for securing.

WHEN AND HOW OFTEN SHOULD YOU CARRY OUT EXERCISES?

It's useful to practise incidents that need both internal and external involvement. Establish a schedule for exercising, and involve agencies that would be expected to take part. So you might agree to practise:

- Major incidents every 5 years (with external agencies)
- Site wide incidents every 2 years (up to board level participants)
- Incident room exercise once a year
- Table top external exercise every 2 years (with CTSA involvement, no wider agencies)
- Table top incident room once every 6 months (internal participants only)

Table top exercises are a useful way to practise scenarios in a secure environment, and they can help people to perform better when faced with a real incident. Always monitor table top exercises in real time.

HUMANS ARE NOT ALWAYS LOGICAL

So it's a good idea to test scenarios where the unexpected happens, and in different circumstances, such as:


1. Busy periods
2. Operations systems at full load
3. Operations systems at half load
4. Different phases of a constructions period


Practice with Gold and Silver command structures so that security officers understand the reporting routes and are comfortable with this type of communication.


Bronze responsibilities include tactical roles; silver is more procedural. Usually this means that supervisors contact bronze counterparts, and the head of security communicates at silver level.


Always keep a log of the training: this will list actions and decisions taken (and any gaps encountered).

It's a good idea to practise post incident events such as report writing, investigations and lessons learnt from time to time.


 You may also want to read about [Follow-up after exercises and incidents](#)

 You may also want to read about [Use case: overview](#)


 You may also want to read about [Threat: overview](#)

 You may also want to read about [Staff training](#)


 You may also want to read about [Incident response plan: overview](#)

 You may also want to read about [Resilience: overview](#)

 You may also want to read about [Maintenance and repair](#)

 Go to [5. Exercising](#)

 Go to start of [Control Rooms Guidance](#)

 Go to [Glossary](#)



Follow-up after exercises and incidents

Training exercises are also an opportunity to examine any gaps in procedure or technology. It's important to combine this with a culture of no blame, as this can be an effective way to maintain robust systems.

Always follow up after you've carried out an exercise, simulation, table top exercise or other event.

Everyone benefits from a learning culture: the feedback you get can highlight gaps in procedures or pinpoint where training is needed.

Debriefs after the exercise/simulation help people to reflect on and learn from incidents. They can help to improve future responses.

Examine the log of the exercise/simulation: this will list any gaps encountered, and inform any actions that are needed to remedy them. Then in the debrief you can discuss communication issues or staffing issues that may have arisen.

Assess the training: you can use standard operations procedures for this.

DID ANY EQUIPMENT SHOW UP AS FAULTY?

1. Make sure that maintenance and repair teams get a prioritised list of items that need immediate attention, such as the CCTV / tech systems.
2. Report any technology glitches to manufacturers.



You may also want to read about [Use case: overview](#)



You may also want to read about [Post-incident debriefs](#)



You may also want to read about [Maintenance and repair](#)



You may also want to read about [Incident response plan: overview](#)



You may also want to read about [Staff training](#)



Go to [5.Exercising](#)



Go to start of [Control Rooms Guidance](#)



Go to [Glossary](#)



Glossary, acronyms and abbreviations

Here we explain some of the terms used in CPNI's Control Rooms Guidance.

AACS Automated Access Control Systems	An electronic or electro-mechanical system that requiring the entry of personal identification information before allowing access to people/vehicles/objects to a site. Access is only granted if this information matches data on the list of authorised users.
Ambient temperature	The air temperature of an environment or object. The air temperature around computing equipment should be 16-24 degrees Celsius.
Anti-passback	A security mechanism that prevents an access card/device being used more than once without its exit being registered by the system – so an entrance card cannot be shared by two people entering the site at the same time.
ARC Alarm receiving centres	Off-site monitors of alarms and CCTV systems across multiple sites. The centres filter activations to prevent unnecessary responses to false alarms, and they alert the site control room when situations need to be managed.
BMS Building management system	An automated system used to maintain a balanced, efficient and workable climate within the building by monitoring and controlling lighting, temperature and security. Also alerts relevant staff teams when maintenance or other actions are required.
Biometrics	A device to confirm an individual's identity using physiological and/or behavioural measurements.
Bronze Bronze command	The operational tier of command which controls practical response on the ground during the management of an incident. It is the third tier of the Gold / Silver / Bronze structure for response to an emergency or incident.
CCTV Closed circuit television	Cameras linked to monitors for surveillance and security monitoring on a site. The closed circuit limits transmission to a closed group of authorised people.
Comms Communications	
DDA Disability Discrimination Act	UK legislation that makes it illegal to discriminate against an individual with a disability with regard to employment, education, transport, provision of goods, and facilities, premises and services.
Digital footprint	The trail of information left behind whenever you access services online. This might be passive (your personal information collected passively when search engines store your search history) or active (when you share information on blogs or social media).

Double knock system	A system where a security detecting device has to sense two separate events within a set time frame before activating an alarm.
DSM Deputy security manager	
Fenestration obscuration	Blocking the possible view through windows in order to prevent hostile surveillance into the building on a secure site. Generally done by adding window frosting or installing and using blinds.
Gold Gold command	The strategic level of command and control during an incident. At this level policy, strategy and the overall response framework are established and managed for individual agencies responding to the incident. It is the top tier of the Gold / Silver / Bronze structure for response to an emergency or incident.
Haptic Haptic feedback	Feedback from a device which gives the user enhanced information through their sense of touch. For example, a touchscreen mobile phone can be set to vibrate when user touches areas of the screen to register when a button is pressed and a task activated.
HR Hostile reconnaissance	Research and investigation into a site by a person/people with hostile intent, who may use the information to harm the site, the people working there, its assets or reputation.
HSE Health and Safety Executive	The government agency that deals with health and safety at work
IDS Intrusion detection system	A security system which consists of sensors that are able to detect attempts to compromise a secure area
IED Improvised explosive device	A 'home-made' bomb
Ishihara 38 plates	A series of 38 printed circular images to check whether the viewer has full colour vision. Usually in a booklet. Each plate show a circle with coloured dots, and embedded in each circle is a number or pattern of differently coloured dots in the shape of numbers or patterns. Depending on the colour combinations, people with specific types of colour blindness may not be able to distinguish between certain numbers or patterns and the surrounding dots.

Lossless compression	Compression of a digital file (reducing the file size) that does not significantly affect the quality or quantity of the data recovered when the file is unzipped, so all of the data in the file can be restored.
Lossy compression	Compression of a digital file (reducing the file size) that results in a permanent loss of data. This is sometimes acceptable and can be useful when sending a complex image as a .jpg, for example. It's up to the sender to decide which is a priority – reduced file size or retaining the full quality and level of detail of the image.
NPCC National Police Chiefs' Council	
OR Operational requirement	A statement of what a site needs in order to fulfil its aims, with a systematic assessment of possible problems and the solutions required to achieve those aims.
PEN testing Penetration testing	Testing an organisation's information security by using techniques and tools to simulate an attack on that IT system.
PIDS Perimeter intruder detection system	An electronic detection system designed to detect and alert when a site's perimeter is attacked or crossed. Can be either barrier/fence mounted or free standing.
Prox and PIN Proximity card and PIN verification	An access control system that ensures users can only pass through that point if they swipe or present an authorised magnetic card to the reader and enter the correct PIN (personal identification number).
PSA Personal search area	An area where security officers are searching people and their bags
PSIT Physical security over information technology	Protecting IT systems from cyber and other risks.
PTZ Pan-Tilt-Zoom	A type of camera that can be moved and focused by remote control, allowing the image to follow a moving target or scan a wider area.
Quad screen	A CCTV monitor screen showing four images at the same time in four quarters of the screen.
Red teaming	Deploying a team set up specifically to test an organisation's systems and plans. Their purpose is to identify limitations, risks and vulnerabilities which can then inform decision making within the organisation.

Rotakin test	<p>A Home Office-designed test to assess the performance of CCTV security systems. The main aim is to measure whether a site's cameras are capable of producing large enough images of intruders within the video detection zone.</p> <p>Home Office recommended image screen heights (as a proportion of the available screen) are:</p> <p>To detect a moving object or person – 10%; To recognise a moving object or person – 50%; To identify a moving object or person – 100%.</p>
SCR Security control room	
Silver Silver command	<p>This is the tactical tier of command and control within a single agency that co-ordinates the response to an emergency or incident.</p> <p>It is the middle tier of the Gold / Silver / Bronze structure for response to an emergency or incident.</p>
Situational awareness	<p>Being aware of, and understanding, what's going on – and what's the right action to take in this situation (given what you know about it and what your resources are).</p>
Snellen chart	<p>A chart to test how well you can see at a distance ('visual acuity'). It usually shows 11 rows of letters, each row smaller than the one before.</p>
SoP Standard operating procedure	
SM Security manager	
SMS Safety management system	
VBIED Vehicle-borne improvised explosive device	<p>A car bomb (or a bomb on any type of vehicle)</p>
Video analytics	<p>Computerised monitoring and analysis of images on CCTV systems</p>
Vigilance decrement	<p>As people get tired in the course of the work, their attention wanes and they are less likely to detect a person, object or other change in the environment.</p> <p>This 'vigilance decrement' usually happens after 20- 30 minutes of continuous work, depending on the level of concentration required.</p>

 [Go to start of Control Rooms Guidance](#)