CONTROL ROOM DESIGN

SECURING RESOURCES [1]

Building a business case

SETTING UP A CONTROL ROOM [2]

Gaining support

Operational requirement [3]

Equipment [7]

Control room functions [4]

Working environment [6]

Resource mapping [5]

MAINTAINING & ADAPTING [8]

| CCTV system maintenance | Control room review | Workload [9] | Shift patterns [10] | Room conditions [11] |
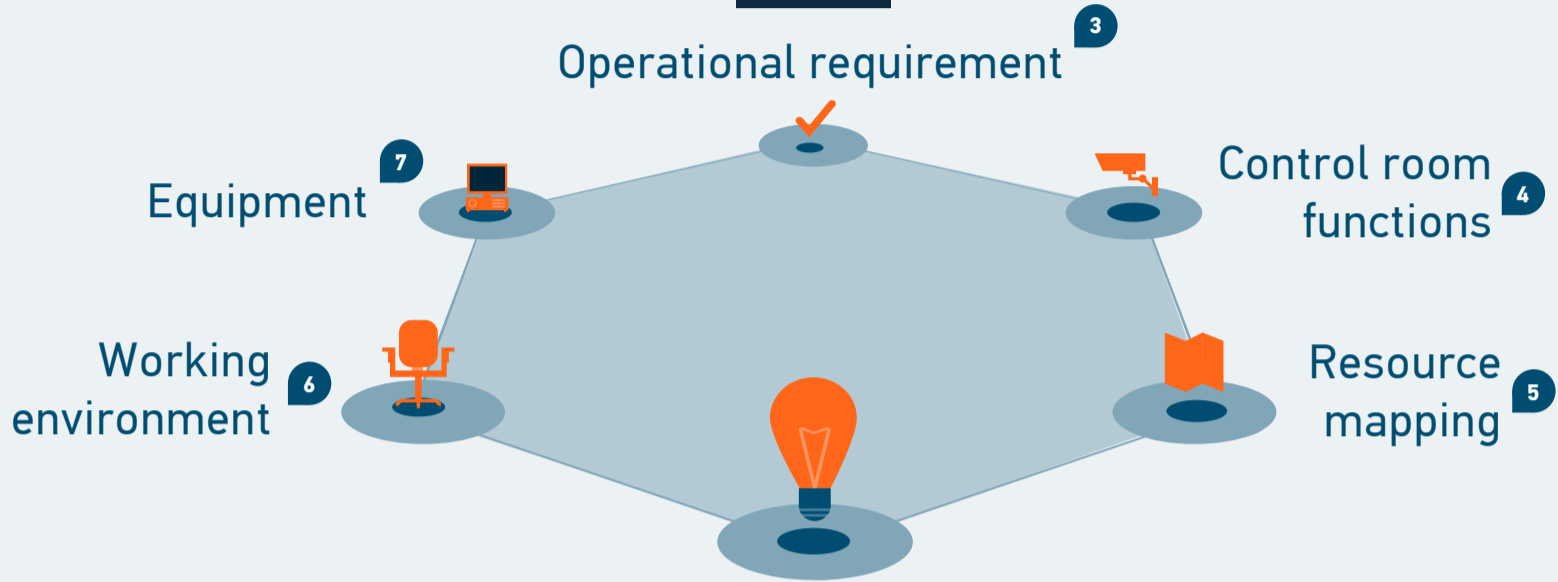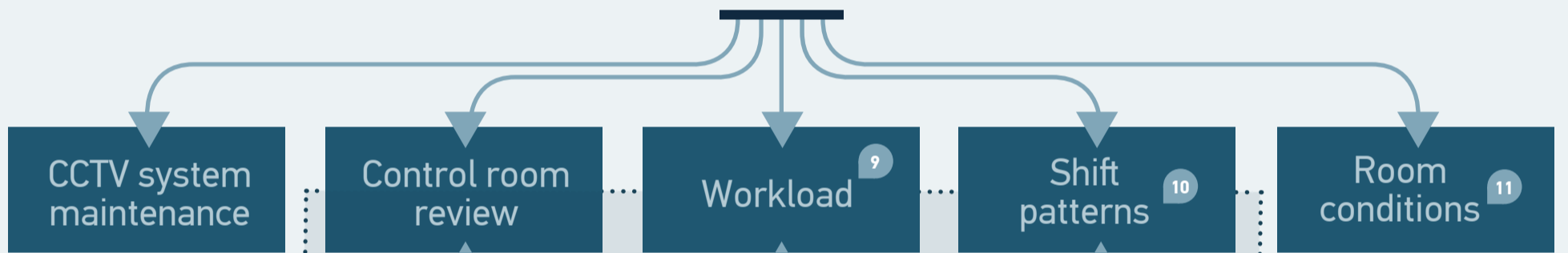
OPERATIONS

MANAGING WORKLOAD [12]

Prioritising security

MULTIPLE FORCES [14]

Monitoring CCTV [13]

CRISIS MANAGEMENT [17]

| Resource mapping [15] | Define overlapping responsibilities | Teamwork [16] | Dedicated space | Communication [18] | Training [19] |

CPNI
Centre for the Protection of National Infrastructure
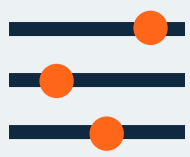
CONTROL ROOM DESIGN AND OPERATIONS

1 SECURING RESOURCES
A set of operational requirements should form the basis of a business case to secure the funds necessary for a security system and security team that is fit for purpose. Planning and justifying the resources required is likely to be important in gaining board-level support.

2 SETTING UP A CONTROL ROOM / CCTV SYSTEM
Important considerations include operational requirements, equipment internal and external to the SOC, staffing and workload, as well as the working environment provided by the control room.

3 OPERATIONAL REQUIREMENT
Crucial for the design (and redesign) of security systems and control rooms, operational requirements should be developed with the input of all key stakeholders. Developing a thorough, bespoke OR should be a priority if you do not have one already.

4 CONTROL ROOM FUNCTIONS
The control room's main function should be security. Non-security responsibilities should be discouraged.

5 RESOURCE MAPPING
Plan how security resources will work together during business as usual and crisis conditions.

6 WORKING ENVIRONMENT
The control room environment should allow staff to remain focussed and comfortable during their working day. Access to the room should be monitored and limited to authorized staff only.

7 EQUIPMENT
Technology should be used to support staff in their work, and the requirements regularly reviewed.

8 MAINTAINING & ADAPTING
Security requirements are likely to change over time, and it is important to assess the changing needs on a regular basis to ensure that the solutions in place are still fit for purpose.

9 WORKLOAD
Workload refers to the total amount of work that a staff member has to do. It is important to consider not only the amount of work, but how challenging individual staff members will find it, considering their skills and abilities.

10 SHIFT PATTERNS
Shift work can have a detrimental effect on wellbeing and performance. This can be limited by designing shift patterns to work with people's natural rhythms and allowing flexibility where possible.

11 ROOM CONDITIONS
The ambient conditions in the control room will affect how comfortable the space is for staff and therefore influence productivity.

12 MANAGING WORKLOAD
Overwork and underwork should be avoided to preserve staff motivation and productivity. Keeping workload at moderate levels will help to reduce the likelihood of staff becoming stressed, bored or making mistakes.

13 MONITORING CCTV
How CCTV feeds will be monitored should be considered when setting up a system or when reviewing it. Considerations include: frequency of monitoring, how long staff should monitor for, rotation of tasks, etc.

14 MULTIPLE FORCES
Many sites have periods where several security teams may share responsibility at certain times. It is important to have clear guidance on areas of responsibility, communications channels and escalation procedures to avoid conflicts.

15 RESOURCE MAPPING
Having a clear map of how the various teams overlap and work with each other is vital for the successful running of a multi-team operation.

16 TEAMWORK
A team can only work effectively if roles are well defined and all team members have a clear understanding of their responsibilities, in both business as usual and crisis conditions.

17 CRISIS MANAGEMENT
Control room setup should allow serious incidents and crisis situations to be handled without compromising the ability to deliver normal security functions. Dedicating a room for the purposes of crisis management is a good place to start.

18 COMMUNICATION
Communication is key when handling a crisis situation. Staff should be aware of the correct channels to use and paths for escalation.
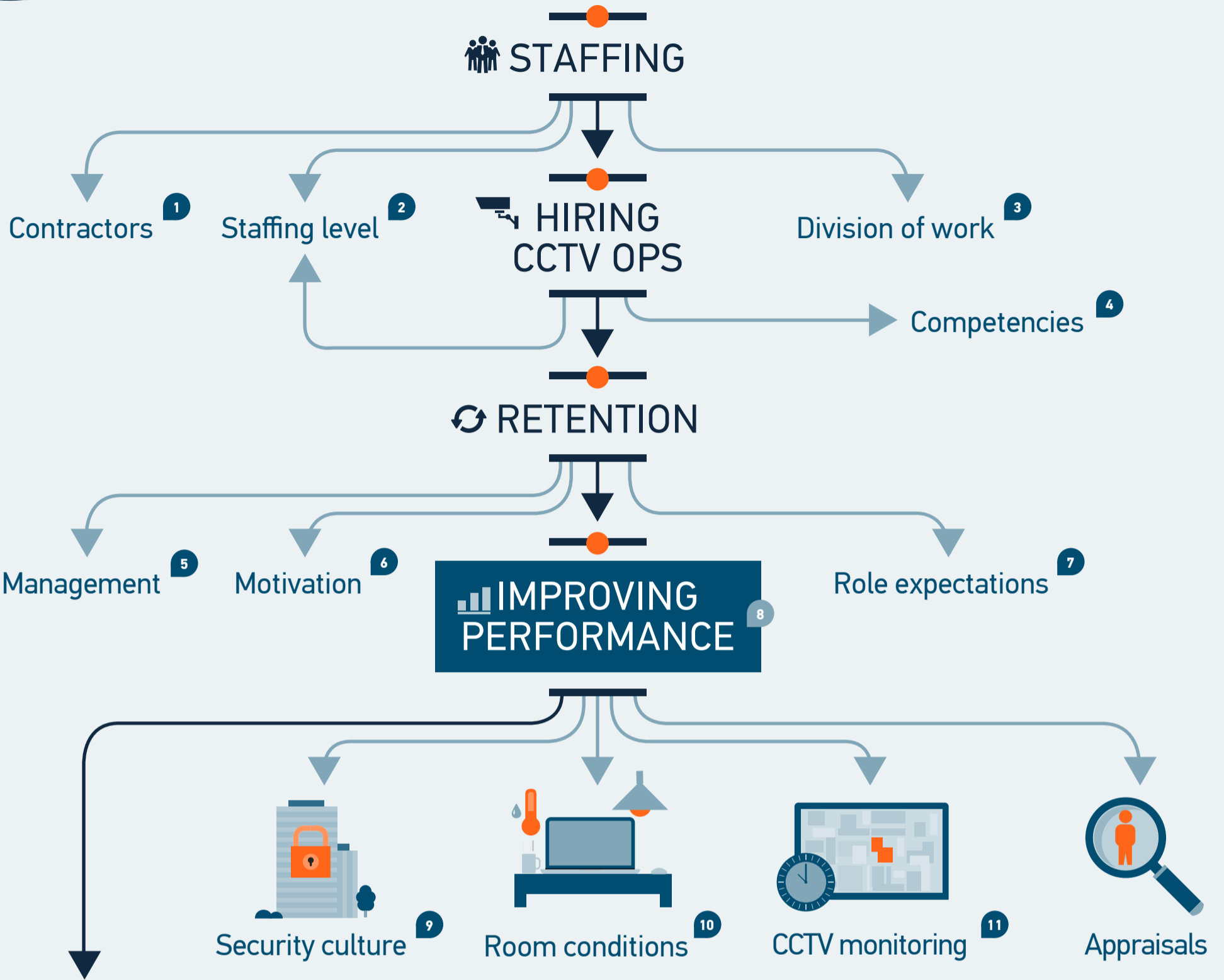
19 TRAINING
Security staff should receive regular training to ensure they have the up-to-date knowledge and skills necessary to do their jobs.
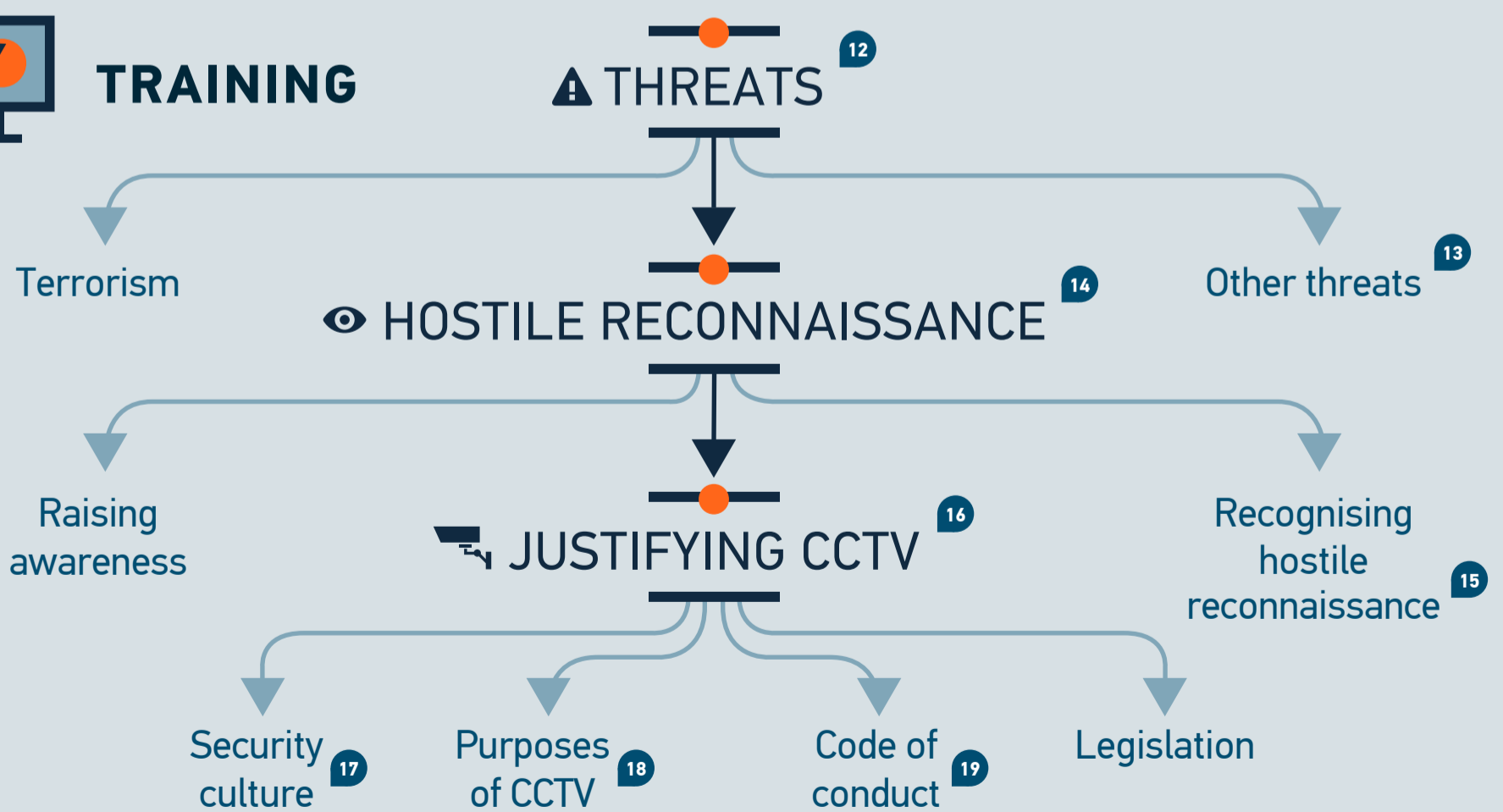
Contact your CPNI Adviser or CTSA for further information

CPNI
Centre for the Protection
of National Infrastructure

STAFFING

STAFFING

Contractors [1] Staffing level [2] **HIRING CCTV OPS** Division of work [3]

Competencies [4]

RETENTION

Management [5] Motivation [6] **IMPROVING PERFORMANCE** [8] Role expectations [7]

Security culture [9] Room conditions [10] CCTV monitoring [11] Appraisals

TRAINING **THREATS** [12]

Terrorism **HOSTILE RECONNAISSANCE** [14] Other threats [13]

Raising awareness **JUSTIFYING CCTV** [16] Recognising hostile reconnaissance [15]

Security culture [17] Purposes of CCTV [18] Code of conduct [19] Legislation

CPNI
Centre for the Protection
of National Infrastructure

STAFFING AND TRAINING

1 CONTRACTORS
Deciding whether to hire contracted or site-employed staff is a key decision when setting up a control room. An employed guard force may be more expensive, but may have higher vetting levels and better understanding of site context.

2 STAFFING LEVEL
The number of CCTV operators required to staff a control room will depend on the activities they are expected to carry out, including non-core security duties - and the technology available to support them.

3 DIVISION OF WORK
Consider how the security duties are divided into roles. You can make the work more interesting and have a better-informed, more motivated workforce through careful design of jobs.

4 COMPETENCIES
A competency specifies the behaviours that staff must demonstrate in order to perform a task to an expected standard. These are helpful in pinpointing the attributes that will be sought when hiring new staff (and aid performance appraisals of current staff).

5 MANAGEMENT
The way in which staff are managed is important for their motivation, work performance and the overall effectiveness of the control room.

6 MOTIVATION
Keeping staff motivated and happy is crucial to ensuring good performance and retaining staff. Motivation can be affected by many factors, including workload, working conditions and management approach.

7 ROLE EXPECTATIONS
Job roles need to be clearly defined, enabling staff to understand where their responsibilities start and end. Mixed roles (e.g. security guard and CCTV operator) can be more interesting for staff, although can also detrimentally impact coverage.

8 IMPROVING PERFORMANCE
The performance of a control room depends on the performance of all staff as individuals and as a team. External factors such as the security culture of the organisation can also play a part.

9 SECURITY CULTURE
Security culture is the overall attitude towards and value placed on security across an organisation. A poor security culture can cause problems for control room performance, if other employees do not observe good security practice.

10 ROOM CONDITIONS
The ambient conditions in the control room will affect how comfortable the space is for staff and therefore influence productivity.

11 CCTV MONITORING
Presentation and procedures for monitoring should be developed with the security requirement in mind. Considerations include the frequency with which a feed should be monitored, and the length of time an operator should spend monitoring CCTV.

12 THREATS
Threats can come from a number of sources. Some sites will be targets in themselves, while others may be at risk if neighbouring sites are targets.

13 OTHER THREATS
Other threats include protestors, extremists and criminals. Establishing the nature of the threat is essential if it is to be dealt with effectively.

14 HOSTILE RECONNAISSANCE
Hostile reconnaissance is the process by which hostiles gather information when planning an attack on a facility or organisation. Identifying and interrupting hostile reconnaissance is key in deterring hostiles and disrupting planned attacks.

15 RECOGNISING HOSTILE RECONNAISSANCE
The context of a facility will affect how easy it is to detect hostile reconnaissance, eg if a site includes a visitor attraction, photography will be commonplace. All staff should be aware of the possibility of hostile reconnaissance.

16 JUSTIFYING CCTV
It may be necessary to change negative attitudes about the need for CCTV and security in general.

17 SECURITY CULTURE
See number 9.

18 PURPOSES OF CCTV
It may be necessary to reassure other employees that CCTV is not there to monitor their activity. In this situation, it can be helpful to explain why CCTV is required, and share examples of what can be captured from any locations of concern.

19 CODE OF CONDUCT
Developing and sharing a clear code of conduct for CCTV usage, review and storage helps security staff understand their responsibilities whilst also reassuring other employees.

Contact your CPNI Adviser or CTSA for further information

CPNI
Centre for the Protection
of National Infrastructure