Highfield Level 2 End-Point Assessment for ST1016 Professional Security Operative

End-Point Assessment Kit

Pathway: Security Control Room Operative

Highfield Level 2 End-Point Assessment for ST1016 Professional Security Operative – Security Control Room Operative

EPA Kit

Contents

Please click on the headings below to navigate to the associated section of the EPA Kit.

How to use this EPA Kit

Welcome to the Highfield End-Point Assessment Kit for the Professional Security Operative apprenticeship standard.

Highfield is an independent end-point assessment organisation that has been approved to offer and carry out the independent end-point assessments for the Level 2 Professional Security Operative apprenticeship standard. Highfield internally quality assures all end-point assessments in accordance with its IQA process, and additionally all end-point assessments are externally quality assured by the relevant EQA organisation.

The EPA Kit is designed to outline all you need to know about the end-point assessments for this standard and will also provide an overview of the on-programme delivery requirements. In addition, advice and guidance for trainers on how to prepare apprentices for the end-point assessment is included. The approaches suggested are not the only way in which an apprentice may be prepared for their assessments, but trainers may find them helpful as a starting point.

Highfield also offers the Highfield Professional Security Operative Apprenti-kit that is a comprehensive learning resource, which is designed to be used on-programme.

For more information, please go to the Highfield Products website. Please note that the use of this kit is not a prerequisite for apprentices undertaking the Professional Security Operative end-point assessment.

Key facts

Apprenticeship standard:	Professional Security Operative
Pathway:	Security Control Room Operative
Level:	2
On-programme duration:	Minimum of 12 months
End-point assessment window:	3 months
Grading:	Pass/merit/distinction
End-point assessment methods:	Knowledge test
	Observation with questions
	Professional discussion

In this kit, you will find:

- an overview of the standard and any on-programme requirements
- a section focused on delivery, where the standard and assessment criteria are presented in a suggested format that is suitable for delivery
- guidance on how to prepare the apprentice for gateway
- detailed information on which part of the standard is assessed by which assessment method
- suggestions on how to prepare the apprentice for each part of the end-point assessment
- a section focused on the end-point assessment method where the assessment criteria are presented in a format suitable for carrying out 'mock' assessments

Introduction

Standard overview

A professional security operative protects people, assets, property and premises. They are an organisation's first line of defence against activities that threaten the security of the UK. They are on the front line and act as an ambassador for the security profession and the organisation in which they work. Employment can range from a small front of house security team to large scale nationwide organisations. Specific responsibilities will vary, but the knowledge, skills and behaviours needed by employees will be the same regardless of the role.

Key responsibilities are likely to include identifying the risk of the security of people, -places, property and assets, identifying suspicious items, conducting regular and random searches and reporting and recording information following organisational procedure.

This standard offers 4 specialisations: operational security operative, cash and valuables in transit operative, mobile security patrol operative and security control room operative. This kit is centred on the security control room operative pathway. This is a role that specialises in controlling and monitoring security systems in real time, such as CCTV.

On completion, apprentices may choose to register as a member with the International Foundation for Protection Officers.

This apprenticeship also aligns with The Security Institute for 2 routes:

- an apprentice without prior experience in the sector can apply for membership at a non-professional grade.
- an apprentice with relevant work experience, along with industry related level 3 and above qualifications may meet the criteria for a professional membership grade.

On-programme requirements

Although learning, development and on-programme assessment is flexible, and the process is not prescribed, the following is the recommended baseline expectation for an apprentice to achieve full competence in line with the Professional Security Operative apprenticeship standard.

The on-programme assessment approach will be agreed between the training provider and employer. The assessment will give an ongoing indication of an apprentice's performance against the final outcomes defined in the standard. The training provider will need to prepare the apprentice for the end-point assessment, including preparation for the observation and professional discussion.

The training programme leading to end-point assessment should cover the breadth and depth of the standard using suggested on-programme assessment methods that integrate the knowledge, skills and behaviour components, and which ensure that the apprentice is sufficiently prepared to undertake the end-point assessment. Training, development and ongoing review activities should include:

- achievement of level 1 English and maths. If the apprentice began their apprenticeship training before their 19th birthday, they will still be subject to the mandatory requirement to study towards and achieve English and maths. The requirements for English and maths are optional for apprentices aged 19+ at the start of their apprenticeship training.
- completion of a portfolio through which the apprentice gathers evidence of their progress.
- completion of an Emergency First Aid at Work qualification.
- study days and training courses.
- mentoring/buddy support.
- regular performance reviews undertaken by the employer.
- structured one-to-one reviews of their progress with their employer and/or training provider.

The apprentice must complete a minimum of **12 months** on-programme training. During this time, they will work to meet the knowledge, skills and behaviours outlined in this EPA Kit.

Use of Artificial Intelligence (AI) in the EPA

Where AI has been used as part of the apprentice`s day-to-day work and forms part of a project report, presentation, or artefact, it should be referenced as such within the work. AI must not be used to produce the report or portfolio.

Where AI has been used as part of a portfolio that underpins an interview or professional discussion or any other assessment method, it should be fully referenced within the portfolio.

Additional, relevant on-programme qualification

There is 1 mandatory qualification apprentices must complete for this standard. This is Emergency First Aid at Work. Apprentices will need to achieve a one-day Emergency First Aid at Work qualification that is regulated by Ofqual or conforms to Health and Safety Executive (HSE) guidelines.

Readiness for end-point assessment

For an apprentice to be ready for the end-point assessments:

- the apprentice must have achieved Level 1 English and maths. The requirements for English and maths are mandatory for all apprentices aged between 16-18 at the start of their apprenticeship training. The requirements for English and maths are optional for apprentices aged 19+ at the start of their apprenticeship training.
- the apprentice must have passed the Emergency First Aid at Work qualification.
- the apprentice must have gathered a portfolio of evidence against the required elements to be put forward to be used as the basis for the professional discussion.
- the apprentice must have gathered their organisation's policies and procedures as requested by Highfield. For guidance, a list of examples has been provided below.
    - Equality, diversity and inclusion
    - Dealing with prohibited items
    - Completing documentation and reports
    - Completing welfare checks
    - Reporting of incidents and errors
- this list is not definitive. The policies and procedures may already be included as part of the portfolio of evidence.
- the line manager (employer) must be confident that the apprentice has developed all the knowledge, skills and behaviours defined in the apprenticeship standard and that the apprentice is competent in performing their role. To ensure this, the apprentice must attend a formal meeting with their employer to complete the **Gateway Readiness Report**.
- the apprentice and the employer should then engage with Highfield to agree a plan and schedule for each assessment activity to ensure all components can be completed within a 3-month end-assessment window. Further information about the gateway process is covered later in this kit.

If you have any queries regarding the gateway requirements, please contact your EPA Customer Engagement Manager at Highfield Assessment.

Portfolio of evidence requirements

The apprentice must compile a portfolio of evidence during their time on-programme that is mapped against the knowledge, skills and behaviours assessed in the professional discussion.

Evidence sources for the portfolio may include:

- workplace documentation and records
- workplace policies and procedures
- witness statements
- annotated photographs
- audio recordings
- video clips with a maximum total duration of 15 minutes and where the apprentice must be in view and identifiable

This is not a definitive list and other evidence sources are possible. The portfolio should not include reflective accounts or any methods of self-assessment. Any employer contributions should focus on direct observations of performance rather than opinions.

The portfolio of evidence will typically contain **10 discrete pieces of evidence**. Evidence may be used to demonstrate more than 1 knowledge, skill or behaviour.

The portfolio must be accompanied by a **portfolio matrix.** This can be downloaded from our website. The portfolio matrix must be fully completed, including a declaration by the employer and the apprentice to confirm that the portfolio is valid and attributable to the apprentice.

The portfolio of evidence must be submitted to Highfield at gateway. It is not directly assessed but underpins the professional discussion. The assessor will review the portfolio in preparation for the assessment. Feedback on the content of the portfolio will not be provided.

Order of end-point assessments

There is no stipulated order of assessment methods and the result of one assessment does not need to be known before starting the next. This will be discussed with the apprentice, training provider and/or employer with our scheduling team when scheduling the assessments to ensure that the learner is provided with the best opportunity to attempt the assessment.

Click here to return to contents

The Highfield approach

This section describes the approach Highfield has adopted in the development of this end-point assessment in terms of its interpretation of the requirements of the end-point assessment plan and other relevant documents.

Documents used in developing this end-point assessment

Professional Security Operative standard 2023

https://www.instituteforapprenticeships.org/apprenticeship-standards/professional-security-operative-v1-0

End-point assessment plan (2023 ST1016/v1.0)

https://www.instituteforapprenticeships.org/apprenticeship-standards/professional-security-operative-v1-0?view=epa

Specific considerations

Highfield's approach does not deviate from the assessment plan.

Click here to return to contents

Gateway

How to prepare for gateway

After apprentices have completed their on-programme learning, they should be ready to pass through 'gateway' to their end-point assessment.

Gateway is a meeting that should be arranged between the apprentice, their employer and training provider to determine that the apprentice is ready to undertake their end-point assessment. The apprentice should prepare for this meeting by bringing along work-based evidence, including:

- customer feedback
- recordings
- manager statements
- witness statements

As well as evidence from others, such as:

- mid and end-of-year performance reviews
- feedback to show how they have met the apprenticeship standards while on-programme

In advance of gateway, apprentices will need to have completed the following. The requirements for English and maths listed below are mandatory for all apprentices aged between 16-18 at the start of their apprenticeship training. The requirements for English and maths listed below are optional for apprentices aged 19+ at the start of their apprenticeship training.

- Achieved Level 1 English
- Achieved Level 1 maths
- Compiled a portfolio of evidence
- Submitted any policies and procedures requested by Highfield
- Passed Emergency First Aid at Work qualification

Therefore, apprentices should be advised by employers and providers to gather this evidence and undertake these qualifications during their on-programme training. It is recommended that employers and providers complete regular checks and reviews of this evidence to ensure the apprentice is progressing and achieving the standards before the formal gateway meeting is arranged.

The gateway meeting

The gateway meeting should last around an hour and must be completed on or after the apprenticeship on-programme end date. It should be attended by the apprentice and the relevant people who have worked with the apprentice on-programme, such as the line manager/employer or mentor, the on-programme trainer/training provider and/or a senior manager (as appropriate to the business).

During the meeting, the apprentice, employer and training provider will discuss the apprentice's progress to date and confirm if the apprentice has met the full criteria of the apprenticeship standard during their on-programme training. The **Gateway Readiness Report** should be used to log the outcomes of the meeting and agreed by all 3 parties. This report is available to download from the Highfield Assessment website.

The report should then be submitted to Highfield to initiate the end-point assessment process. If you require any support completing the **Gateway Readiness Report**, please contact your EPA Customer Engagement Manager at Highfield Assessment.

Please note: a copy of the standard should be available to all attendees during the gateway meeting.

Reasonable adjustments and special considerations
Highfield Assessment has measures in place for apprentices who require additional support. Please refer to the Highfield Assessment Reasonable Adjustments policy for further information/guidance.

ID requirements
Highfield Assessment will need to ensure that the person undertaking an assessment is indeed the person they are claiming to be. All employers are, therefore, required to ensure that each apprentice has their identification with them on the day of the assessment so the end-point assessor can check.

Highfield Assessment will accept the following as proof of an apprentice's identity:

- a valid passport (any nationality)
- a signed UK photocard driving licence
- a valid warrant card issued by HM forces or the police
- another photographic ID card, such as an employee ID card or travel card

Click here to return to contents

Professional Security Operative apprenticeship standard

Below are the knowledge, skills and behaviours (KSBs) from the standard and related assessment criteria from the assessment plan. On-programme learning will be based upon the KSBs and the associated assessment criteria are used to assess and grade the apprentice within each assessment method.

Knowledge test
Knowledge and skills
Legislation, regulation, and procedures
K11 Security industry regulators and associations **and the role they play** **K16 Principles of equality, diversity, and inclusion** and the impact on the organisation **K20 Check calls** and **welfare check procedures** for **lone workers**
Communication and customer service
K23 Working securely online (including password management) and **recognising suspicious communication** such as email, websites, social media, pop-ups
Security incident response
K18 How to identify suspicious items and activities, and the principles of **HOT and the 4C's** **K19 Why items are prohibited** and **how to identify** them **K22 Prohibited articles** relevant to assignment instructions and **how to deal with them**
Security operations
K13 The principles, processes, and **technology for controlling access into an area**
Security technology and equipment
K21 The importance of operating **body worn cameras in** the appropriate setting and according to **organisational requirements**

K27 Methods to mitigate gaps in **physical security measures** using **monitoring equipment**
Security control room operative
K55 Importance of calibrating control room equipment
Skill
Security operations
S16 Identify the component parts of **explosive and incendiary items**, firearms, and other **prohibited items**
Amplification and guidance

- **Security industry regulators and the role they play:**
  - The main regulator in the security industry is the Security Industry Authority (SIA), they:
    - regulate compulsory licensing of individuals who undertake designated activities
    - manage a voluntary approved contractor scheme, which measures private security service suppliers
    - are regulated by the Home Office
  - British Security Industry Association (BSIA):
    - the trade association for the professional security industry in the UK
  - The Security Institute:
    - a UK-based professional body for security professionals
    - membership of the institute is open to security professionals and those interested in security

- **Principles of equality, diversity, and inclusion** may include:
  - Equality legislation defines 9 protected characteristics:
    - age
    - sex
    - religion or belief
    - pregnancy and maternity
    - marriage and civil partnership
    - disability
    - race

        - sexual orientation
        - gender reassignment
    - Organisations must ensure that they are compliant with equality laws when employing individuals and ensure that they do not directly or in directly discriminate
    - Equality in an organisation means ensuring that everyone has the same opportunities
    - Diversity in an organisation brings a broad range of ideas, skills and qualities
    - 'Legitimate aim' is the genuine non-objective reason behind the discrimination such as a security officer refusing someone who is under the age of 18 entry into a nightclub
    - Everything is determined by the Human Rights Act. There are 3 main categories that are used to categorise the articles that the act covers:
        - absolute (cannot take the right away)
        - limited (can be limited in specific circumstances)
        - qualified (can be balanced against the rights of the public or public safety)

- **Check calls:**
    - check calls are done to ensure that a staff member who is working alone is safe and well at that given time
    - they will be carried out if determined to be a requirement under a risk assessment
    - if a lone worker does not answer the check call a colleague should be sent to check their welfare
    - the recommended period of time between check calls is an hour

- **Welfare check procedures** may include:
    - Asking staff to contact a control room every hour
    - Control room contacting staff members every hour
    - Automated messaging systems to declare they are alive and well with response activations if not completed
    - GPS tracker systems that can be monitored in real time
    - Internet technology which allows staff to 'drop pins'
    - 24/7 outsourced control room which can answer SOS button activations
    - Site visits by mobile supervisors

- **Lone workers**:
  - staff members who work by themselves without close or direct supervision
  - employers should assess the risk of lone working within their organisation, and then implement measures to keep staff safe, such as a check call procedure

- **Working securely online:**
  - it is important to take steps to keep data, information and staff safe while using the internet and social media sites.
  - actions to encourage this include:
    - using two-factor authentication to add extra security to online accounts
    - ensuring that software is kept up to date and security updates are installed regularly to minimise security vulnerabilities
    - using password managers and strong password management practices
    - backing up data to external or cloud-based storage in case devices are lost, stolen or damaged so that the data can be restored
    - never posting about the organisation an operative works for on their personal social media
    - complying with the General Data Protection Regulations (GDPR)

- **Recognise suspicious communication** by:
  - being wary of unsolicited emails, text messages and pop ups
  - checking the validity of email addresses
  - checking the sender of the information
  - being aware of phishing attempts

- **HOT and the 4Cs:**
  - the risk of terrorism in the UK is set by the National Counter Terrorism Security Office (NaCTSO), and our internal risk assessment should take this into account
  - the 4Cs principle is where security officers should start:
    - Confirm:

  - must first confirm that the unattended item is in fact suspicious. We can do this be initially asking member of the public who the item belongs to. If the item remains unclaimed, then we can initiate the HOT protocol.
- HOT:
  - hidden - has someone deliberately tried to conceal it from view?
  - obviously suspicious - does its appearance seem odd or out of the ordinary? Is it showing wires, batteries or liquids?
  - typical - is it typical for the location? For example, a large rucksack would be expected at an outdoor festival but would be out of place at an indoor concert venue.
- Usually, you will be able to use your judgement to define whether the item is HOT. If you believe that it is HOT, then you can move to the remaining 'C's.
- Clear:
  - clear the area. Do not touch the item. Take charge and move people away to a safe distance. Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out. Keep yourself and other people out of line of sight of the item.
  - hide behind something such as a hardened cover and keep away from glass such as windows and skylights
  - cordon off the area.
- Communicate:
  - inform supervisors or management team and follow the escalation procedure. However, radios should not be used within 15 metres of the item. It may also be your responsibility to call the emergency services.
- Control:
  - control the area by ensuring no one gets close to the item. This can be done by placing hazard warning tape around the item at the appropriate distance. Reasonable force can be used to keep people safe, although strict conflict management principles should be followed and hands on should be a last resort.
  - try to keep eyewitnesses on hand so they can tell the police what they saw.

- The reason **why items are prohibited** is usually related to the following:
  - safety and public interest, such as glass bottles may be prohibited in a venue because of the safety risk they pose
  - the integrity and operational success of the business
  - the venue does not want the item on their premises
  - the item is not allowed but is not illegal, such as fireworks and alcohol

- **How to identify** prohibited items:
  - when carrying out searches at a venue, certain items will be prohibited which means that the person will not be allowed to enter while in possession of them

- **Prohibited articles** can be split into many categories. These can include:
  - controlled substances:
    - identified by their look and the circumstances
    - these are illegal items and illicit drugs such as Class A, B and C substances
  - weapons made for causing injury:
    - these are items that are made for causing injury such as knifes, daggers and batons
    - items that go against the Prevention of Crime Act 1953 and the Criminal Justice Act 1988
  - adapted or intended weapons:
    - these are items which are either intended to cause harm or adapted to cause harm
    - examples include baseball bats, screwdrivers, pens, car keys, bottles, chairs and tables
  - a venue may consider other items that are not otherwise illegal prohibited in their venue:
    - these are not illegal items, but the site or event has determined them as prohibited
    - examples include alcohol, umbrellas, food, phones, cameras, bags over a certain size, hats and jackets

- **How to deal with them** depends on the circumstance and type of prohibited item but some options may include:
  - the item would be surrendered by the customer and then confiscated according to the confiscation procedure. The customer may be allowed to enter or remain.
  - in certain circumstances the customer could choose not to surrender the item, and simply exit the situation.
  - the item could be surrendered and confiscated, and the person could be asked to remain, be detained or arrested.
  - security staff have no legal or statutory right to search someone without permission, under no circumstances can a person forcibly be searched, and depending on their locality (Scotland, England, Northern Ireland or Wales) there may be different arrest powers for possession of drugs and weapons, and this should always be done in line with their employer's arrest policy and procedure.
  - in any of these scenarios the security officer should follow their reporting and escalation procedures.

- prohibited items that have been abandoned should be secured by the operative and reported.
- suspicious items or substances should be reported to the relevant person.

- **The principles, processes for controlling access into an area:**
  - access control is the process of determining and enforcing who has access to buildings, grounds, equipment, and sensitive areas
  - the main principle of access control is that only authorised individuals can enter certain restricted areas
  - access control goes beyond securing the premises from criminals, it also prevents employees from entering restricted areas such as those containing sensitive chemicals, equipment or data

- **Technology for controlling access into an area:**
  - access control systems are used to control access to areas, therefore, protecting people, assets, and the site itself
  - card readers are used to scan information from user credentials to grant access to individuals
  - an advantage of having electronic forms of individual access is that they can immediately be disabled
  - access control systems consist of 2 main components: hardware and software
    - Hardware includes the physical components such as access cards, controllers and readers
    - Software allows credentials to be assigned to people so that they have the correct access to specified areas
  - access control heavily relies on techniques like authentication and authorisation, which allow organisations to explicitly verify both that users are who they say they are and that these users are granted the appropriate level of access based on context such as device, location and role

- **Body worn cameras** are used to record interactions between operatives and the public, and can be an effective tool for improving safety, accountability for all involved

- **Organisational requirements:**
  - it is crucial that cameras are used in a way that is consistent with the law and organisational policies
  - body worn cameras must be clearly visible when in use
  - cameras must only be used when necessary and the organisation states

- they must be used in a way that is respectful of the privacy and dignity of the people being recorded
- the camera does not replace the need to complete documentation such as incident reports
- according to the United Kingdom College of Policing, the use of body-worn cameras should be clearly advertised, and the cameras should be used with reasonable discretion
- the wearer does not require a CCTV operator licence, but the images must be downloaded by an authorised person
- images must be stored securely on an approved system, and the principles of the Data Protection Act apply:
  - storage limitation
  - accuracy
  - data minimisation
  - purpose limitation
  - processed lawfully, fairly and in a transparent manner
  - security, integrity and confidentiality
- the owner (business) of the camera must have approval with the Information Commissioners Office (ICO) to use this equipment, and the storage system and length of storage is stated on the ICO approval

- **Physical security measures** are crucial to protect people, property, and assets from harm and damage. Traditional physical security measures include locks, gates and security guards. Gaps in physical security measures can be mitigated by:
  - implementing key card access control systems
  - installing security cameras in key areas
  - adding motion detectors to the inside of properties
  - physically seeking identification from individuals

- **Monitoring equipment** can be used to mitigate gaps in physical security measures. This may include:
  - access control systems:
    - used to limit access to authorised individuals and resources
    - can be used to restrict access to sensitive areas of a facility and monitor behaviours and movements
  - motion detectors:
    - used to detect movement in a facility

        - they can be used to trigger alarms or alert security personnel when unauthorised movement is detected
        - they can also be used in conjunction with other monitoring equipment such as video surveillance and temperature sensors
    - video surveillance:
        - an effective way to monitor and record activities in a facility
        - it can be used to detect and deter criminal activity, monitor employee behaviour, and identify potential security breaches
        - it can also be used in conjunction with other monitoring equipment such as motion detectors and temperature sensors
    - temperature or heat sensors:
        - used to monitor the temperature in a facility
        - they can be used to detect fires, overheating equipment and other potential hazards
        - it can also be used in conjunction with other monitoring equipment, such as video surveillance and motion detectors
    - alarm systems:
        - used to alert security personnel when a security breach is detected
        - they can be used to detect unauthorised entry, motion or temperature changes
        - they can be used in conjunction with other monitoring equipment, such as video surveillance and motion detector

- **Calibrating control room equipment** is crucial as it:
    - ensures accurate readings and data – many control room systems rely on sensors, monitors and alarms that provide crucial data inputs. If any of those are out of calibration, it can lead staff to making decisions based on inaccurate information.
    - avoids false alarms and unnecessary responses - improperly calibrated sensors or thresholds can trigger false alarms. This results in wasted staff time responding to phantom issues and alarm fatigue if it is constantly happening.
    - supports reliability of critical systems – security control centres often oversee important infrastructure such as CCTV and alarm response. Calibrated tools are essential for monitoring the health and performance of these critical systems.
    - ensures compliance with regulations and standards – this helps to avoid regulatory fines or licence issues.
    - optimises system performance - proper calibration keeps tools and technologies working at peak accuracy and efficiency.
    - provides accurate situational awareness and system reliability.

- **Importance of calibrating** CCTV:
    - ensures that systems are aligned to the same time and date for accuracy and evidentiary requirements.

- ensures video clarity and coverage – if cameras are out of focus, have colour balance issues, or are positioned incorrectly, video footage will lack the quality and coverage needed to serve its purpose.
- avoids blind spots or gaps in coverage - over time, building settling, weather events, or inadvertent bumps can shift cameras out of alignment creating monitoring blind spots (regular calibration avoids this).
- supports video analytics performance – many CCTV systems run video analytics like motion detection, object tracking, facial recognition, calibrating the cameras is key for these features to work properly.
- allows accurate display mapping – control room video walls need calibrated cameras maps so security staff can quickly orient to events happening on specific cameras. Out of date mapping creates delays or confusion.
- adheres to industry standards and best practice for CCTV system operation – regulations such as BS EN 62676-4 provide calibration specifications that should be followed.

- **Identifying prohibited items:**
  - it is vital that a security officer can recognise what is 'normal' and what is not in their place of work - this will help them to identify what is abnormal and therefore may be suspicious
  - security officers should use the HOT protocol (hidden, obviously suspicious, typical)
  - if in any doubt the security officer should contact their supervisor and seek further guidance
  - if a security officer finds an item or substance to be suspicious to them, they must trust their instincts and report it immediately to the relevant person within their organisation
  - assignment instructions will advise of any items which are prohibited on the site and the procedures to be followed, should they be found or declared

- **Explosive and incendiary items:**
  - Improvised explosive devices (IED) can be made from many different materials and substances, therefore, there is no fail-safe guide to be able to identify all components of an IED or firearm
  - IEDs are created using everyday items and substances
  - Recognised items that are often used in explosive items include, wire, a trigger, a power source, an explosive charge and an initiating mechanism
  - Gasoline and fuses are commonly associated with incendiary items

- When identifying the components of firearms, operatives will typically look for cartridge cases

Communication and customer service		
Knowledge	**Skills**	**Behaviours**
K12 The importance of communications and **its impact on** customer service, **the organisation** (including subversive activity) and its stakeholders **K14** Methods to **identify the needs of others** and **communication strategies** for different situations **K15** How to use **communication methods and technology systems** to enable appropriate work and statutory information to be recorded or transmitted (for example, technology and methods for handover)	**S7 Deliver customer service** to all stakeholders, **responding to the needs of the individuals** **S10** Use **digital communication applications** and information management systems to communicate, learn**, share, and record information** **S12** Use verbal and non-verbal **communication skills** (for example **the 'Power of Hello'**) when interacting with individuals **S13 Use an appropriate tone of voice** in all communications that reflect the organisations or client's values **S15 Defuse potential conflict situations**	**B2** Be **professional, calm and positive role model** to others in attitude to work **B4 Respectful to colleagues and stakeholders** always **B5 Act reliably and responsibly** **B6 Committed to continued professional development (CPD)** to maintain and enhance competence and share learning with others **B8 Build appropriate working relationships** and **respect boundaries**. Be co-operative and flexible

Observation with questions
To pass, the following must be evidenced
CC1 Communicates respectfully with stakeholders using verbal and non-verbal means to establish a rapport and deliver customer service (K12, K14, S7, S12, B4) **CC2** Acts responsibly to diffuse potential conflict situations by communicating in a calm and professional manner with others in a way that reflects the organisation's values (S13, S15, B2, B5)
To gain a distinction, the following must be evidenced
CC3 *Adapts their language and behaviour, in a calm and professional manner, in response to individual needs to exceed stakeholder expectations* (K12, K14, S7, S12, B2)
Professional discussion
To pass, the following must be evidenced
CC4 Explains how they use digital communication systems to record and share information for statutory and security purposes, in line with legislation and organisational procedure (K15, S10) **CC5** Describes how they demonstrate a commitment to CPD, how they share this learning with others in a cooperative manner and how this can benefit the organisation (B6, B8)
To gain a distinction, the following must be evidenced
CC6 *Evaluates the importance of following guidance and procedures in the use of digital communication applications and information management systems and the possible impact on the individual, and organisation, if these are not followed* (K15, S10)
Amplification and guidance

• **The importance of communication:**
  ○ it is important to tailor and adapt communication styles to each customer, such as:
  ▪ younger customers tend to favour digital channels like text and social media

        - older customers often still prefer phone conversations and emails
        - some individuals prefer short and direct communication while others want more detail and conversation
    - poor communication can lead to bad customer service and health and safety issues

- **Its impact on the organisation:**
    - by developing effective communication strategies, organisations can ensure that they meet the needs of their stakeholders, customers and staff. This can:
        - encourage repeat business
        - create returning custom
        - create new business
        - encourage a buy in from staff
    - organisations should empower employees to handle enquiries in a thoughtful and empowered way, using soft skills and emotional intelligence
    - the needs and expectations of the customer should be balanced with the organisation's values and goals

- **Identify the needs of others** by:
    - choosing the correct means of communication, leading to better customer relationships
    - understanding the receiver's style and preference
    - listening actively, being empathic and being mindful of tone and body language

- **Communication strategies** and **skills** include:
    - verbal:
        - information is exchanged using words spoken out loud
    - written:
        - information is wrote down on paper or typed out using technology
        - when using this method tone of writing and selection of words is crucial to ensure the reader gets the information right
    - non-verbal:

        - information is transferred through gestures, posture, tone of voice, and eye contact
    - visual:
        - information is displayed through signs, drawings, illustrations and pictures
        - this method is often used to support both verbal and written communication to make information more understandable

- **Communication methods and technology systems**:
    - methods to record, communicate and share information between colleagues and stakeholders:
        - emails
        - reports
        - daily occurrence books
        - notebooks
    - methods to share information immediately:
        - radios
        - face-to-face
        - telephone
        - loudspeakers
    - communication should be accurate, brief and clear
    - when information is recorded the General Data Protection Regulation (GDPR) should be adhered to

- **Deliver customer service** by:
    - being responsive to concerns and requirements
    - being proactive and empathetic
    - listening actively, recognising the needs of the customer and their concerns
    - understanding the customer's perspective and providing a solution
    - treating customers with dignity and respect even if they are angry or upset - by doing this, the situation can be diffused and potentially prevent further escalation

- **Responding to the needs of the individuals** by:
  - being responsive, promptly responding to your customer's complaints, queries, questions and feedback
  - having a thorough understanding of the products and services offered so the correct information, advice or guidance can be given to customers
  - providing a personalised service by relating to the specifics of the customer's situation and avoiding generic responses

- **Digital communication applications** are used to exchange information, messages and ideas using digital technologies and platforms. Some of these include:
  - text messages
  - emails
  - internet messaging systems
- these applications can make information more accessible to staff working in remote areas or lone workers

- **Shar**ing **and record**ing **information:**
  - when using applications to record information the General Data Protection Regulation (GDPR) must be adhered to
  - all information that is recorded must be correct, comply with legislation and provide a clear audit trail of an incident

- **The 'Power of Hello':**
  - it is a technique used when initially approaching a customer.
  - By speaking to someone, it gives an opportunity not only to demonstrate good customer service but to show that we are attentive, and observant of the customer's/visitor's needs.
  - this can also demonstrate to those with bad/criminal intentions that they have been observed and can alter their behaviour. It may make them feel wary and vulnerable, making them less likely to continue with malicious plans at the location.

- **Use an appropriate tone of voice:**
  - people often pay more attention to tone and body language than the words that are said

- when communicating with clients or customers, it is important to use a tone of voice that is respectful and professional
- avoid emotionally charged language, being calm and thoughtful influences the customer to do the same
- mastering tone with customers is an ongoing journey that requires self-awareness, empathy and alignment with company values

- **Defuse potential conflict situations:**
  - people often become frustrated if they feel something is not going their way. This may be because they do not understand one of the rules or the reasons for it and may not wish to accept a decision that has been made. Steps to take to diffuse conflict may include:
  - listening actively:
    - give the customer full attention and focus, don't interrupt or jump to conclusions.
  - showing empathy:
    - let them know that their frustrations have been recognised and that they will be resolved together.
  - owning the situation:
    - take responsibility of the issue, regardless of where fault lies.
  - finding the root cause:
    - ask thoughtful questions to understand all the underlying factors that are causing the customers dissatisfaction.
  - presenting solutions:
    - offer options, alternatives and solutions focused on resolution. Set appropriate expectations.
  - thanking the customer:
    - however the interaction concludes, thank the customer for their time and feedback.

- Be **professional, calm and** a **positive role model** by:
  - maintaining a positive attitude in the workplace
  - encouraging optimism and implementing ideas that contribute to a positive environment
  - using and promoting encouraging language
  - being respectful and courteous to colleagues and customers
  - demonstrating accountability

- Be **respectful to colleagues and stakeholders** by:
  - treating co-workers and leaders courteously and fairly
  - valuing their beliefs, contributions and ideas
  - respecting everyone in the workplace, no matter their role
  - behaving in this way prevents conflict, fosters a positive culture and enables cooperation

- **Act reliably and responsibly** by:
  - being punctual and ready to work with the correct mindset
  - completing tasks on time
  - following the organisation's policies and upholding its values
  - following legislation and regulations to prevent harm to others and self
  - promoting security, safety and service
  - behaving in this way builds trust among the public, encourages respect and promotes professionalism

- Being **committed to continued professional development (CPD):**
  - Shows a commitment to ongoing learning and development of skills and understanding
  - Refreshes and updates knowledge in line with current legislation and regulation
  - This can be done by:
    - completing courses
    - watching others in the profession
    - attending workshops and lectures
    - sharing and discussing this learning with others to encourage development in the workplace
  - CPD fosters:
    - up-to-date knowledge
    - enhanced skill sets
    - advanced career prospects
    - alignment with industry standards

- **Build appropriate working relationships** by:
  - being cooperative and flexible
  - being respectful, honest and transparent
  - listening actively and communicating effectively

- **Respect boundaries** by:
  - understanding what is appropriate in a situation
  - avoiding behaviour that could be perceived as inappropriate or unprofessional
  - adapting to circumstances

Security operations		
Knowledge	**Skills**	**Behaviours**
K3 Impact of reputational damage for the **individual**, **organisation**, and security industry **K9** The **movements and behaviours** of people **K10 Awareness of working environment** and areas **K24 Negative impact** of allowing certain behaviours, items or objects into certain areas and the **reputational damage** they may cause	**S1 Follow assignment instructions** relevant to operational duties **S6** Challenge suspicious activities on or around the site and apply **SCaN** principles (see, check, and notify) **S8 Navigate a site plan or map** of their working environment and areas	**B1 Be vigilant**, always **pay**ing **close attention to detail** **B7 Follow employer's or client's code of conduct** relating to behaviour, appearance and conduct

K25 The unique threats and risks across a wide range of sites or locations **K26 Dynamic Risk Assessments** for visits to a site or location	**S9 Carry out observation of designated areas, report and record any irregularities** mitigating security and safety threats **S11** Use **personal protection equipment (PPE)** correctly **S14 Contribute to review and improve** the daily operating **processes and procedures** **S17 Carry out dynamic risk assessments** at sites or locations	
Observation with questions		
To pass, the following must be evidenced		
SO1 Navigates a site plan and assesses risk at the site or location by carrying out an observation of the designated area, and reporting and recording any irregularities to the site risk assessment (K26, S8, S9, S17) **SO2** Follows the assignment instructions and the clients or employers code of conduct and policies for behaviour, appearance, and the use of PPE (S1, S11, B7) **SO3** Identifies and challenges suspicious activity across sites and locations, in line with SCaN principles, by being vigilant and aware of the area, and the movements and behaviours of people (K9, K10, K25, S6, B1)		
To gain a distinction, the following must be evidenced		
SO4 *Uses their knowledge of the site and usual movement and behaviour of people to recognise and check anomalies, showing awareness of the possible implications of these, reporting in line with procedures* (K25, K26, S17, B1)		

Professional discussion
To pass, the following must be evidenced
SO5 Explains how they contribute to the review and improvement of processes and procedures to support organisational improvement and how these reviews minimise the risk of reputational damage by improving the removal of certain items, objects or behaviours in particular areas (K24, S14) **SO6** Explains how allowing some behaviours or items in certain areas can have a negative impact on the organisations reputation, why this is important, and how they contribute to improving processes and procedures (K3, K24, S14)
To gain a distinction, the following must be evidenced
No distinction criteria
Amplification and guidance
• The **impact of reputational damage** on **individuals** may include: ○ a loss of trust, credibility and respect from peers and colleagues ○ a significant impact on the individual's personal and professional life due to a loss of income and future employment ○ short or long-term reputational damage depending on the severity • The **impact of reputational damage** on **organisations** may include: ○ a loss of business, as clients may lose confidence in the ability of the security provider to protect them and their assets ○ a loss of credibility, trust and revenue ○ short or long-term reputational damage depending on the severity • The **movements and behaviours** of individuals should be monitored as: ○ behavioural detection can be used as a first line defence in countering threats ○ recognising movement patterns can help in early detection of anti-social behaviour ○ these are key in identifying threats at the earliest opportunity

- Having an **awareness of** the **working environment**:
  - having a comprehensive understanding of the area of work will help to identify potential threats
  - it is crucial to check all areas of the environment for any damage and security breaches
  - by assessing employees' awareness, organisations can adapt their policies and training programmes to accommodate to the constantly changing threat landscape
  - being aware of 'what looks right' will help employees when completing patrols, lock-up checks and movement around the site

- The **negative impact**s may include:
  - feeling a lack of safety by those working or using the area socially
  - a negative perception of the area
  - people avoiding the area
  - the level of impact may depend on the behaviour or item, for example, someone bringing a weapon into the area, or demonstrating loud, aggressive behaviour towards the occupants
  - a loss of trust if service users see unruly, illegal, or dangerous behaviour go unchallenged

- **The unique threats and risks:**
  - each location, site and workplace bring their own unique risks, depending upon the sector that the business sits, will determine the types of threats and risks, but these typically include:
    - threats - burglary, theft, criminal damage, terrorist attacks, industrial espionage, physical or verbal assaults
    - risks - lone working, mental health of employees and general health and safety risks such as slips, trips and falls

- A **dynamic risk assessment** is a continuous safety practice that allows officers to quickly identify and analyse risks and hazards, on the spot and remove them if possible. They:
  - are completed with the information gained at the time so decisions are made in real time and done 'on the spot'
  - are usually carried out by workers as a situation, job, or location changes to be able to identify risks that were not covered in the formal risk assessment
  - should complement and fill in any gaps that could not be predicted when completing a standard risk assessment

- do not replace formal risk assessments that are prepared in advance

- **Follow**ing **assignment instructions:**
  - it is crucial to read and understand the assignment instructions for the role
  - the assignment instructions will have a list of duties and potentially a timescale
  - ensure that all duties are carried out as described and any incidents, issues or alarms are recorded and reported in the correct way

- **SCaN:**
  - See, check and notify (SCaN) aims to help organisations maximise safety and security using their existing resources
  - This principle empowers staff to correctly identify suspicious activity and what to do when they encounter it
  - It helps to ensure that individuals or groups seeking to cause an organisation harm are unable to get the information they need to plan their actions
  - It can also help to disrupt threats that may originate from inside an organisation
    - See – recognise what is normal and what is not, and to be vigilant of suspicious behaviour
    - Check – use the 'power of hello' and friendly conversation to find out if the activity is suspicious or not
    - Notify – know how and when to report suspicious activity, and what to do if it is reported to them by another individual

- **Navigate a site plan or map** by being able to:
  - demonstrate an understanding of the layout of the site and use a map to plan a route to another area, or to demonstrate to a site visitor the route they need to take
  - find and plan a route to a destination requested by a third party
  - consider any accessibility issues

- **Carry out observation of designated areas:**
  - officers will be expected to conduct regular and random searches

- monitoring the assigned areas to act as a deterrent, identify hostile reconnaissance, identify suspicious items, people, or vehicles, and respond to alarms, incidents, and emergencies

- **Report and record any irregularities:**
  - any irregularities or breaches to security must be reported following site instructions
  - officers must be able to demonstrate the procedure to do this and have knowledge of the reporting process to be completed

- **Personal protection equipment (PPE)** is dependent upon the site requirement, but the following may be issued:
  - waterproof clothing
  - high-visibility clothing
  - headwear
  - gloves (needle/slash resistant)
  - rubber gloves
  - face-shields
  - stab-resistant vests
  - ear defenders
  - eye protection
  - safety footwear
  - these should all be worn correctly, stored appropriately and checked prior to use

- **Contribute to review and improve processes and procedures:**
  - if staff have an idea which would improve practices or support the service delivery, then they should put this forward to their manager
  - managers should also speak to staff and gain an insight into their role and encourage suggestions for improvement

- **Carry out dynamic risk assessments:**
  - dynamic risk assessments follow the formal risk assessment steps

- if an officer recognises a risk, they need to ensure that the correct procedures are followed to ensure a safe working environment

- **Be vigilant** and **pay close attention to detail** by:
  - not falling into a state of unconscious incompetence
  - carrying out duties in line with security procedures and reporting any breaches

- **Follow employer's or client's code of conduct** by:
  - wearing the correct attire – uniform should be clean and worn in the correct manner with no additions or substitutions
  - adhering to and promoting the employer's/client's values and beliefs
  - behaving in a professional and courteous manner
  - promoting safety, security and service

Security technology and equipment	
Knowledge	**Skills**
K4 The **security systems, applications, technology, and equipment** used, **how to identify faults or errors** and the remedial action to take	**S3 Use security systems**, applications and software, technology and equipment **in line with organisational and operational requirements**
Observation with questions	
To pass, the following must be evidenced	
ST1 In line with organisational procedures, uses security systems, applications, and technology to support security operations, and identifies faults with equipment taking remedial action where necessary (K4, S3)	

To gain a distinction, the following must be evidenced
No distinction criteria
Amplification and guidance

- **Security systems, applications, technology, and equipment:**
  - on commencing duty, staff should run through checks of the systems to ensure that they are working correctly
  - systems should be routinely checked to ensure that they are working and operating as required – for some systems this is carried out by the manufacture of their representatives
  - maintenance should be documented and carried out on a regular basis

- **How to identify faults or errors:**
  - any faults or issues should be reported following the on-site procedure
  - staff may be alerted to faults in the system by alarms, either visual or audio
  - appropriate actions to take may include:
    - identifying the problem – where it is and what it is, depending on the system the staff will be alerted, and a check of the system should be made to confirm the fault
    - depending on the system, there may be a back-up power facility process, and staff should be aware of this and how to implement, if not automatically done
    - contacting engineers and making a fault report
    - making an entry into the operator log - this will demonstrate if there is a pattern to the faults, which could highlight nefarious activity
    - if access control fails manually managing entry – keeping a written record of any people or vehicles that enter or leave the site

- **Use security systems in line with organisational and operational requirements** by:
  - logging all system access and data queries conducted during shifts to maintain auditable logs
  - using communication, monitoring and recording equipment solely for legitimate public safety purposes
  - supporting IT teams in scheduled security platform maintenance by reporting issues and seeking updates on known issues
  - keeping up to date with best practices and legislative changes

- only using equipment per training guidelines and assignment instructions – this includes adhering to access control polices regrading authorised access

Security patrol, access, and searching – security control room operative pathway	
Knowledge	**Skills**
K54 Importance of checking ID cards and access credentials for control room operatives **K57 The purpose and requirements of virtually searching premises** for control room operatives **K58 Different search methodologies**, techniques, and patterns and why **a search methodology may change** for control room operatives	**S34 Carry out various searches** (for example, of areas, vehicles, or items) from the control room **S35** Apply **control room access control systems**, procedures, and forms of authorisation in **crowded space environments or publicly accessible locations** **S36 Scan and track assigned areas** for control room to control access, detect and respond to unwanted activities, communicate, and report findings
Observation with questions	
To pass, the following must be evidenced	
SP1 Applies control room access control procedures to environments by carrying out searches and checking forms of authorisation, detecting and responding to unwanted activities. Reports findings in line with procedures (K54, K57, K58, S34, S35, S36)	
To gain a distinction, the following must be evidenced	
No distinction criteria	

Amplification and guidance

• **Importance of checking ID cards and access credentials:**
  ○ confirms authorisation:
  ▪ by checking IDs and access cards/badges, security staff can validate that the person attempting to access sensitive areas actually has current and legitimate credentials for that level of access
  ▪ checking identification prevents unauthorised individuals from entering
  ○ upholds access control measures:
  ▪ strict access control policies are vital in high security environments
  ▪ physically inspecting and validating staff credentials before permitting control room entry - maintains robust enforcement of those access policies and acts as a deterrent
  ○ audits access:
  ▪ majority of control rooms require logging or auditing who enters and exits the facility
  ▪ checking identification allows logs to have reliable information on the specific individuals granted entry
  ▪ this supports reviews, investigations or audits of control room traffic
  ○ reinforces cybersecurity practices:
  ▪ many control room credentials also grant access to digital systems
  ▪ confirming an operative's credentials helps cross-check appropriate authorisation for both physical spaces and any sensitive data/controls they may interact with digitally
  ○ data protection compliance:
  ▪ Regulations such as GDPR require data controllers to implement organisational and technical measures, like access controls for those with access to protected information
  ▪ CCTV cameras contain personal information and should not be viewed by unauthorised personnel - routine ID checks supports adherence to such policies
 	
• **The purpose of virtually searching premises:**
  ○ to remotely inspect premises and gather intelligence prior to deploying personnel for on-site operations
  ○ to check anomalies, security issues, hazards (including fire) or other items of interest before sending officers to a location
  ○ it can be used during active incidents in response to remote alarms to assess situations and gain additional visual situational awareness

- the benefits of virtual searches include increased situational awareness, informed deployment of resources, and keeping personnel out of avoidable hazardous situations

- **The requirements of virtually searching premises:**
  - high quality CCTV cameras, ideally with pan, tilt and zoom capabilities
  - stable, high bandwidth connectivity between control room systems and remote camera networks
  - pre-mapped camera presets allowing methodical sweep of designated areas
  - control room visual display screens of adequate size and resolution
  - standardised procedures and checklists for conducting virtual searches
  - note taking and reporting tools to document search findings
  - collaborative software allowing remote specialists to connect for assistance
  - access controls and policy enforcement around permissible search areas

- **Different search methodologies** include:
  - static search:
    - covering designated areas with fixed camera views - used for monitoring known hotspots
  - dynamic search:
    - actively panning, tilting and zooming cameras to sweep wider areas - better for following moving targets or expanding search zones
  - spot-check search:
    - randomly selecting sites or areas to briefly check, then moving to others - useful for general situational awareness
  - pattern search:
    - moving cameras in a pre-planned route to methodically observe a full zone - helps ensure no blind spots or missed areas

- **A search methodology may change** for several reasons, but this may be because of:
  - new intelligence – new information about emerging threats, incidents or persons of interest could alter search priorities
  - ongoing assessments – initial searches may reveal problems requiring follow up such as vandalism or unauthorised access
  - staffing constraints – operator shortages could force transition from proactive wide area searches to shorter spot checks of critical sites

- technical issues – camera, network or system outages may limit search capabilities necessitating adjustments

- **Carry out various searches** by:
  - reviewing search priorities, safety risks, legal restrictions prior to conducting the search.
  - logging operational objectives, location(s), personnel involved into search record documents/system.
  - utilising pre-defined camera presets and past search patterns (if available) for known areas to start.
  - adjusting camera views systematically using full range of pan, tilt and zoom controls. Vary both camera angle and field of view depth during area sweep.
  - adhering to a methodical search sequence to ensure all portions of an area are scanned - zigzag, circular, grid patterns are common. Be sure to check hidden corners/enclosures.
  - if searching vehicles, rotate cameras to capture all angles - underside, wheel wells, trunk, or interior cab. Always look for signs of damage, contraband and stowaways.
  - when searching specific items, utilise maximum optical zoom and adjust lighting to get clear identifiable imagery of the object(s).
  - recording notes, screenshots and video clips during searches to document critical findings. If available utilise collaboration software to get remote specialists involved if needed.
  - after search completion, file detailed reports including any noteworthy observations, actions taken and recommendations for future procedures or area re-inspection.

- **Control room access control systems** to help secure access in such high-traffic environments can include:
  - multiple layer access controls:
    - install a series of access controls, not just a single-entry door
    - options such as employee ID/biometric checks to enter secure wings and corridors prior to reaching the control room itself can enhance the access and egress control
  - mantraps:
    - use multi-door mantrap style vestibules so that public side exterior doors must close before interior doors open to prevent piggybacking behind authorised staff

        - the integration of intercoms and CCTV views of the enclosure will enhance the security
    - rapid-swipe security doors:
        - high speed opening-and-closing automatic doors that open briefly via registered card swipe access - helps avoid unauthorised staff slipping through behind entering employees in crowded environments
    - visitor escorts:
        - require all visitors to be accompanied by an authorised and responsible employee host while visiting control rooms to prevent tampering with equipment or unauthorised access in adjoining areas
    - temporary access badges:
        - issue time-limited credentials for visitors or contractors rather than standard employee access cards
        - includes expiration control and quick disabling of lost badges

- Control rooms in **crowded space environments or publicly accessible locations** such as transportation hubs, stadiums, shopping centres and other publicly accessible locations present unique access control challenges, given the volumes of people circulating in adjoining areas

- **Scan and track assigned areas:**
    - utilise pre-planned camera presets and patrol routes to methodically observe all parts of the designated area - adjust the routes periodically to introduce unpredictability.
    - leverage video analytics (ALARMS) for unusual motion, loitering or perimeter breaches to enhance real-time detection capabilities.
    - actively manipulate PTZ cameras to investigate alerts or visible suspicious behaviours, like vandalism and unauthorised access attempts.
    - maintain constant radio/phone communication with security teams on the ground to coordinate responses to unfolding incidents that require intervention.
    - for lower risk observations like overcrowding or parking violations, logging the time, location details, camera IDs and visual evidence allows later follow-up.
    - throughout monitoring shifts, record thorough yet concise observation logs regarding events, subject descriptions, actions taken - this creates permanent shift records for auditing, reporting and future analysis.

- before shift changes, verbally brief the next operator about ongoing incidents or areas requiring extra attention. Also transfer or escalate written logs to ensure continuity of oversight.
- a security system daily occurrence book – either electronic or paper based can be used for recording information in a formal and timely manner.

Security technology and equipment – security control room operative pathway	
Knowledge	**Skills**
K56 Methods for gathering and storing images (for example CCTV, mobile device recordings, drones) for evidential use for control room operatives	**S38** Identify and use **components of a control room system** **S39 Gather and store CCTV footage** for evidential use
Observation with questions	
To pass, the following must be evidenced	
SE1 Operates the components of a control room system to gather and store images for evidential use, in line with organisational procedure (K56, S38, S39)	
To gain a distinction, the following must be evidenced	
No distinction criteria	
Amplification and guidance	
• **Methods for gathering and storing images** may include: ○ CCTV systems: ▪ high-resolution cameras with features like night vision capability, wide dynamic range, and pan-tilt-zoom functionality ▪ digital video recorders or networked video recorders for capturing continuous footage or clips triggered by motion or alarms	

        - timestamping capability to date and time stamp recordings
        - secure digital storage with automated backups, either onsite or cloud based
        - access controls and audit logs for all video access and downloads
    - Mobile devices:
        - body-worn cameras and phone cameras can be supplements for CCTV cameras
        - secure digital storage is key, often with automated cloud uploads from devices
        - access controls, encryption and flowed audit trails for all mobile video files
        - adherence to GDPR is required
    - Drones:
        - special regulatory clearance and pilot credentials are required
        - registration with local authorities is required
        - high-quality aerial imagery and video capability with geo-tagging, timestamping for all footage
        - secure drone data storage and transmission systems either cloud based or on site
    - Assignment instructions will explain the processes for the following - digitally signing footage, restricted access, backups, and detailed logs of best practices

- **Components of a control room system** includes:
    - operator consoles:
        - this includes desks, computers and software used by human operators to interface with all systems as well as external communications
        - the efficient design is key to control rooms
    - video walls:
        - large multi-display screens showing live video feeds from CCTV cameras, access control systems, and other visual data streams
        - provides situational awareness
    - sensors:
        - inputs from sensors like security alarms, fire detection, air quality monitors, temperature sensors, motion sensors that provide system health, safety and infrastructure monitoring capabilities
    - alarms:

        - audio and visual alarm annunciators that activate emergency response plans, notify staff of detected threats, events or threshold violations in the environment
    - logging recorders:
        - secure locations for servers and databases that accumulate and archive access logs, system-wide audit trails, operator activity logs and reporting
    - communications networks:
        - redundant connectivity like LAN/WAN networks, radio systems linking the control room to personnel, security operations teams and systems in the field
    - backup power:
        - uninterrupted power supply units, standby generators and power distribution units to maintain operation during blackouts

- **Gather**ing **and stor**ing **CCTV footage:**
    - lawful basis:
        - there must be a valid lawful basis for processing and storing the CCTV footage, such as compliance with a legal obligation, legitimate interests, or public interest particularly for evidence in legal proceedings
    - data minimisation:
        - only footage strictly relevant and necessary to the investigation or evidentiary requirement should be stored
    - secure storage:
        - video files containing personal data must be securely stored on secure networks with access control mechanisms and access logging
    - retention periods:
        - clear retention schedules are essential - evidentiary footage and case files should be maintained only as long as investigations or cases are ongoing
        - they must then be securely deleted under 'right to erasure' principles
    - subject access requests:
        - clear procedures must exist to locate and provide copies of stored personal data to individuals legally requesting access to surveillance footage containing them, while redacting others
    - record keeping:

- up-to-date records on location of stored CCTV evidence, investigative use, sharing with authorised parties, retention and eventual destruction should be maintained in a GDPR compliance audit log

Legislation, regulation, and procedures		
Knowledge	**Skills**	**Behaviours**
K1 Relevant industry and operative **specific regulations, legislation, guidance,** and **procedures** (for example assignment instructions, SOPs, EOPs) **K2 The importance of following legislation, monitoring risk,** compliance, control, and the completion of legal documentation **K5 Organisational structure, vision, values,** and **business needs** **K6 Own role within the team**, the **team's role within the organisation** and how it contributes to achieving **organisational objectives** **K17** The **channels to communicate** ideas for **improvement** **K28 Internal** and **external factors** that can affect systems/equipment performance	**S2** Carry out **work in compliance** with all **regulations, guidance, legislation and organisational policies and procedures** **S5** Complete and maintain accurate **documentation or reports** to meet current legislation, guidance, or **organisational requirements**	**B3** Solution-focused **displaying problem solving attributes** **B9 Act honestly** and with integrity

Professional discussion
To pass, the following must be evidenced
LR1 Describes how they apply industry regulation, legislation, guidance, and procedures in their role, acting with honesty and integrity, when monitoring risk and completing security documentation (K1, K2, S2, S5, B9) **LR2** Explains how their role within the team, and their teams role within the organisation contributes to achieving the organisation's objectives, vision, and values (K5, K6) **LR3** Describes the range of internal and external factors that can affect performance of security systems and equipment, and how they have demonstrated a solutions focused approach in communicating ideas for improvement within the organisation (K17, K28, B3)
To gain a distinction, the following must be evidenced
LR4 *Analyses the potential impact of not following industry regulation, legislation, guidance, and procedures on security outcomes, including when monitoring risk and completing security documentation* (K1, K2, S2, S5)
Amplification and guidance

• **Specific regulations** and **legislation:**
  ○ security officers must have a good understanding of the relevant legislation which effects their role, including:
  ▪ The Private Security Industry Act 2001
  ▪ The Human Rights Act 1998
  ▪ The Health and Safety at Work etc. Act 1974
  ▪ Equality legislation
  ▪ The Health and Safety (First Aid) Regulations 1981
  ▪ The Licensing Act 2003
  ▪ General Data Protection Regulation (GDPR)
 	
• **Guidance:**

- security officers should also discuss with their employer what they are being asked to carry out as part of their role. This includes being issued with:
  - assignment instructions
  - risk assessments

- **Procedures:**
  - arrest
  - searching
  - crowd control
  - confiscation policy
  - patrol procedure
  - dealing with electric systems
  - fire evacuation
  - counter terrorism awareness

- **The importance of following legislation:**
  - security officers should ensure that they follow any appropriate legislation which may be relevant to their place of work
  - failure to do so could lead to criminal investigation and/or prosecution, or civil litigation
  - also, a loss of individual or business reputation is likely

- **Monitoring risk:**
  - security staff should always conduct a dynamic risk assessment to assess hazards and remove risks while completing a task. To do this they should:
    - stop the unsafe task
    - immediately report this verbally and in writing to their immediate line supervisor or manager
    - take part in the reporting and investigation process

- always be fair and transparent

- **Organisational structure:**
  - reporting structures are critical to the success of any business and all staff members should know who in their organisation they should be directly reporting to and who they can seek support from
  - a typical business structure will include:
    - group directors, CEOs and managing directors
    - operational directors
    - operational managers
    - area managers
    - area supervisors
    - site supervisors
    - team leaders
    - officers

- **Vision, values:**
  - security officers should be aware of and have a clear understanding of adhering to the vision of the company they are working for, and how that might specifically affect their daily role
  - the values and needs of a company should be made available to security officers through the employee handbook and assignment instructions

- **Business needs:**
  - employers must balance the needs of staff members and the needs of the business at the same time, such as granting several staff members annual leave at the same time when the company has a contractual requirement to meet

- **Own role within the team:**
  - security officers should understand how they 'fit' into the team and the overall structure of the organisation, such as identifying individual strengths and weaknesses, recognising tasks they complete, and acknowledging how colleagues can be supported

- **Security team's role within the organisation:**
  - security teams are often made up of permanent staff who work together all year round
  - teams will be given a specific direction to work within the organisation's vision

- **Organisational objectives:**
  - within a company's vision there will be defining objectives - these will be a set of standards which the team must adhere to and actively work towards achieving
  - the following documentation may drive these standards:
    - assignment instructions
    - employee handbook
    - risk assessments
    - company policies

- **Channels to communicate** include:
  - Written reports
  - Incident logs
  - Emails
  - Calls/texts
  - Duty registers
  - GPS tracking systems
  - Health and safety incident reports

- **Improvement:**
  - employers are responsible for assessing and improving any practice or procedures, therefore, it is crucial for employees to communicate any improvements they deem necessary, for example, reporting incidents

- **Internal factors** include:
  - poorly trained staff
  - staff unable to adhere to system and equipment operating procedures
  - poorly implemented procedures
  - hardware failure due to poor maintenance
  - staffing and human resources issues

- **External factors** include:
  - power outage
  - cyber-attack
  - incidents such as a power cut or fire evacuation
  - overcrowding which leads to internet failure
  - criminal incident increase in area which causes a resource pull on CCTV systems and reporting

- **Work in compliance:**
  - officers must ensure that all work tasks are completed to standard and to the satisfaction of the employer and client

- **Regulations, guidance, legislation and organisational policies and procedures:**
  - an officer's work should comply with the following:
    - Health and Safety Regulations, for example, wearing the correct PPE, and using equipment correctly

- General Data Protection Regulation – following data and security policies to prevent data breaches
- Health and Safety (First Aid) Regulations 1981 – responding correctly to medical issues, threats to life and knowing how to deliver first aid
- The SIA Code of Conduct – all SIA holders must adhere to this, as breaching the code can result in a loss of licence

- **Documentation or reports:**
  - should be completed to comply with the General Data Protection Regulation, which includes keeping personal information secure and confidential
  - evidence and audit trails should be sound
  - officers should have clarity on how information is passed from one party to another

- **Organisational requirements:**
  - all paperwork should be accurate and clear

- **To display problem solving attributes** security officers are expected to behave in the following way:
  - positive communication on approaching the customer
  - assertive non-verbal and verbal communication
  - greet the customer
  - actively listen to the problem
  - maintain a calm and confident manner
  - provide options and offer potential solutions to the issue
  - build rapport
  - use de-escalation techniques

- **Act honestly** by**:**
  - a security officer should act honestly at all times by doing the following:
    - not accepting bribes
    - being transparent with the customers and the client
    - not making false promises

Security incident response	
Knowledge	**Skills**
K7 Methods for **identifying weapons** (for examples explosive and incendiary items, firearms, bladed weapon) and other prohibited items that can cause security risks **K8 Emergency** procedures, **incidents and disruptions** that may occur in a security environment and the appropriate action or **reporting process** to take in the event of an incident	**S4 Take action** in the event of an **incident, disruption, alarm activation or emergency,** liaising with relevant people, escalating when necessary and recording actions and outcomes to meet guidance or organisational requirements
Professional discussion	
To pass, the following must be evidenced	
SI1 Describes the methods for identifying weapons and other prohibited items, and how to apply these methods in line with organisation procedure (K7) **SI2** Explains how they apply organisational procedures in the event of an incident or emergency, the actions they take in response and how they ensure the relevant people are engaged (K8, S4)	

To gain a distinction, the following must be evidenced
SI3 *Justifies their response to an incident or emergency, and how they ensured public safety in rapidly changing circumstances* (K8, S4)
Amplification and guidance

- **Identifying weapons:**
  - searches can be conducted on site which will act as a means of identifying items - these may be either illegal, or prohibited under the admissions policy of the venue
  - depending on the specific site assignment instructions and risk assessment, a number of methods can be employed to identify these

- **Methods** include:
  - self - searching - a softer approach which ensures compliance with a search standard, but also works to help disprove any possible allegation which may be placed against the staff member.
  - bag searches - it is best practice to ask customers to empty the contents of their bag onto a table. This combines the self-search with a bag search. Staff should be very careful when dealing with people's possessions and should not place their hands into someone else's bag.
  - pat down searches - this is the only element of a search where a staff member would be required to put their hands on a customer. This should be done systematically, usually from head to toe, and should not differ from person to person.
  - advanced search methods – usually involve a piece of equipment or a secondary resource, such as:
    - Handheld metal detectors - the use of a 'wand' to detect metal
    - X Ray scanners – used for detecting particular compounds, for instance, organics, electric or metal
    - Archway metal detectors - a 'walk through' scanner which picks up on various compounds including metal and organic material
    - Additional resources such as a canine unit to search for explosives and incendiary materials

- **Emergency** types:
  - incidents which occur on a site can vary widely, depending on the risk presented at that specific and particular event or site, and the possible impact factors which may affect behaviour
  - emergencies, incidents and disruptions can be classed as:
    - emergency, urgent or non-urgent

        - crime or non-crime
        - for example, there could be a fire on site which is big enough to cause major disruption - this fire could also be classed as a crime if arson is suspected

- **Incidents and disruptions** include:
    - fire
    - power cut
    - flood
    - chemical spillage
    - terror incident
    - fight
    - gas leak

- The **reporting process** to follow, depending on the circumstance but it typically involves:
    - preserving the scene and ensuring no one tampers with evidence
    - contacting the emergency services that are appropriate to the risk
    - informing your supervisor or line manager
    - taking action to prevent further harm
    - liaising with the in-house response teams, and adhering to the possible escalation procedures
    - dealing with the public, and ensuring smooth flow of pedestrians and possible members of the public

- Take action in the event of an **incident** by:
    - assess its position within the law hierarchy, for instance, is it a crime or a civil matter?
        - if it is a crime, is it common law or statutory?
        - if non-crime, what is the specific site procedures for dealing with this? For example, a fire evacuation.
    - security officers should get a clear understanding of the incident management plan before beginning shift - this could be via e-learning, toolbox talks or onsite briefing.

- Take action in the event of a **disruption** by:
  - immediate assessment of the disruption should take place to determine the following:
    - who is at risk?
    - is there any risk to life?
    - is a crime taking place? If so, what power of arrest do we have?
    - is there a serious disruption to the operations of the venue?
    - is there a requirement to call the emergency services?
    - do we need police support, or do we have our own internal response team who can assist?

- Take action in the event of an **alarm activation or emergency** by:
  - security officers should be expertly familiar with the procedure of how to respond to the activation.
  - fire regulations now dictate that certain criteria should be met, such as the number of individuals who attend the fire panel. There may be a requirement for security staff to attend the fire panel with management and attempt to locate and confirm the fire is genuine. There are also regional procedures too. For example, in Scotland, fire services will not attend unless you are confirming a real fire.

- **Take action** by doing the following (these are paramount):
  - act to preserve life, where it is safe to do so
  - liaise with supervisors and management on the smooth running of operations
  - preserve evidence
  - control the area
  - complete the incident reports fully and accurately

Security incident response – security control room operative pathway
Skills
S37 Deploy correct type of **barrier** in a control room context safely
Professional discussion
To pass, the following must be evidenced
SR1 Describes incidents that have required a barrier to be deployed, how they determined the correct type of barrier and how they ensured it was deployed correctly and in line with organisational procedures (S37)
To gain a distinction, the following must be evidenced
No distinction criteria
Amplification and guidance
• **Deploy**ing **barriers** is an important physical security measure for control room to restrict and control access. Several types can be used safely and effectively: ○ retractable bollards: ▪ robust vehicle barrier placed surrounding buildings, and outdoors to prevent unauthorised vehicle approach near entry points ▪ they are hydraulically activated, powered by electricity or back-up generators ○ security gates/turnstiles: ▪ located at personnel entrances to serve as an access control checkpoint, able to detect valid credential swipes ▪ should have intrusion alarm triggers, rapid operation to allow swift entry/exit ○ lockable security door: ▪ used alongside access control readers as a secondary physical barrier to prevent control room entry ▪ choose fire code compliant doors that delay/deter intruders but allow emergency exit ▪ ensure appropriate staff have keys/credentials at all times to avoid impediments to urgent access ○ lifts: ▪ remote operations to lock at certain floors

- consider if passengers are inside when locking lift
- operatives should always consider the power source, operational use and emergency response when deploying barriers

Click here to return to contents

Assessment summary

The end-point assessment for the Professional Security Operative apprenticeship standard is made up of **3** components:

1. A knowledge test consisting of **40** multiple-choice questions of **60-minute** duration
2. A **90-minute (+10%)** observation followed by **30-minutes (+10%)** of questioning, which will include a minimum of **5 questions**
3. A **60-minute (+10%)** professional discussion underpinned by a portfolio of evidence, of at least **8 questions**

As an employer/training provider, you should agree a plan and schedule with the apprentice to ensure all assessment components can be completed effectively.

Each component of the end-point assessment will be assessed against the appropriate criteria laid out in this kit, which will be used to determine a grade for each individual. The grade will be determined using the combined grades.

Knowledge test

All assessment methods are weighted equally. Total marks available are 40.

- To achieve a **pass**, apprentices will score at least 28 out of 40
- To achieve a **distinction**, apprentices will score 36 and above
- **Unsuccessful** apprentices will have scored 27 or below

The test may be delivered online or be paper-based and should be in a 'controlled' environment.

Observation with questions

Apprentices will be marked against the pass and distinction criteria outlined in this kit.

- To achieve a **pass**, apprentices must achieve **all** of the pass criteria
- To achieve a **distinction**, apprentices must achieve **all** of the pass criteria and **all** of the distinction criteria
- **Unsuccessful** apprentices will have **not** achieved all of the pass criteria

The observation with questions must take place in the apprentice's normal place of work, for example, their employer's premises or a customer's premises.

Professional discussion

Apprentices will be marked against the pass and distinction criteria outlined in this kit.

- To achieve a **pass**, apprentices must achieve **all** of the pass criteria
- To achieve a **distinction**, apprentices must achieve **all** of the pass criteria and **all** of the distinction criteria
- **Unsuccessful** apprentices will have **not** achieved all of the pass criteria

The professional discussion may be conducted using technology such as video link, as long as fair assessment conditions can be maintained.

Grading

Grades from individual assessment methods must be combined to determine the overall EPA grade. The apprenticeship includes pass, merit and distinction overall grades.

To achieve a **pass**, the apprentice must achieve a pass in all the assessments.

To achieve a **merit**, the apprentice must achieve a distinction in 2 assessments.

To achieve a **distinction**, the apprentice must achieve a distinction in all the assessments.

The overall grade for the apprentice is determined using the table below:

Knowledge test	Observation with questions	Professional discussion	Overall grading
Fail	Any grade	Any grade	**Fail**
Any grade	Fail	Any grade	**Fail**
Any grade	Any grade	Fail	**Fail**
Pass	Pass	Pass	**Pass**
Distinction	Pass	Pass	**Pass**
Pass	Distinction	Pass	**Pass**
Pass	Pass	Distinction	**Pass**
Pass	Distinction	Distinction	**Merit**
Distinction	Distinction	Pass	**Merit**
Distinction	Pass	Distinction	**Merit**
Distinction	Distinction	Distinction	**Distinction**

Retake and resit information

If an apprentice fails an end-point assessment method, it is the employer, provider and apprentice's decision whether to attempt a resit or retake. If a resit is chosen, please call the Highfield scheduling team to arrange the resit. If a retake is chosen, the apprentice will require a period of further learning and will need to complete a retake checklist. Once this is completed, please call the Highfield scheduling team to arrange the retake.

The resit is normally expected to take place after all the required assessments have been taken and the individual assessment results and overall apprenticeship result has been given to the apprentice.

A resit is typically taken within **3 months** of the EPA outcome, and a retake is dependent on how much retraining is required but it is typically taken within **4 months** of the EPA outcome.

Failed assessment methods must be resat or retaken within a **6-month** period from the EPA outcome, otherwise the entire EPA will need to be resat or retaken.

Resits and retakes are **not** offered to an apprentice wishing to move from a pass to a higher grade.

The apprentice will get a maximum EPA grade of pass for a resit or retake, unless there are exceptional circumstances that are beyond the control of the apprentice as determined by Highfield.

Click here to return to contents

Assessing the knowledge test

The knowledge test will consist of **40** multiple-choice questions and last **60 minutes**. The pass mark is **28** out of **40** and the distinction mark is **36** out of **40**.

The test will consist of:

- **35** core questions
- **5** security control room operative pathway questions

The apprentice will have **at least 5 days'** notice of the date and time of the test.

The knowledge test may be delivered online or be paper-based and should be taken in a controlled and invigilated environment. The test is closed book which means that the apprentice cannot refer to reference books or materials.

Before the assessment

The employer/training provider should:

- brief the apprentice on the areas that will be assessed by the knowledge test.
- in readiness for end-point assessment, set the apprentice a mock knowledge test. A test is available to download from the Highfield Assessment website. The mock tests are available as paper-based tests and also on the mock e-assessment system.

Knowledge test KSB's

Knowledge test
K11 Security industry regulators and associations and the role they play
K13 The principles, processes, and technology for controlling access into an area
K16 Principles of equality, diversity, and inclusion and the impact on the organisation
K18 How to identify suspicious items and activities, and the principles of HOT and the 4C's
K19 Why items are prohibited and how to identify them
K20 Check calls and welfare check procedures for lone workers
K21 The importance of operating body worn cameras in the appropriate setting and according to organisational requirements
K22 Prohibited articles relevant to assignment instructions and how to deal with them
K23 Working securely online (including password management) and recognising suspicious communication such as email, websites, social media, pop-ups
K27 Methods to mitigate gaps in physical security measures using monitoring equipment
K55 Importance of calibrating control room equipment
S16 Identify the component parts of explosive and incendiary items, firearms, and other prohibited items

Click here to return to contents

Assessing the observation with questions

The assessor will observe the apprentice in their workplace completing their day-to-day duties under normal working conditions and ask questions. Simulation is not allowed. The assessor will only observe 1 apprentice at a time.

The apprentice will have **2 weeks'** notice of the observation with questions.

The observation with questions will last a total of **2 hours**, with **90 minutes** for the observation followed by **30 minutes** allocated for questions. The assessor can increase the time by up to **10%** to allow the apprentice to complete a task or respond to a question.

The observation with questions may be split into discrete sections held on the same working day, which is to accommodate for breaks and moving between locations. Breaks will not count towards the total assessment time.

The assessor will explain to the apprentice the format and timescales of the observation with questions before it starts. This briefing will not be included in the assessment time.

The observation with questions must take place in the apprentice's normal place of work, for example, their employer's premises or a customer's premises. The equipment and resources needed for the observation must be provided by the employer and in safe working condition.

The following activities must be observed during the observation:

- communicating with stakeholders
- using various equipment while carrying out their duties
- following instructions for security operations
- following procedures in the event of an incident
- completing appropriate documentation
- operating control room equipment
- conducting searches

Questions will be asked after the observation to assess the apprentice's breadth and depth of competence against the grading criteria. As only naturally occurring work will be observed, the criteria that the apprentice did not have chance to demonstrate will be assessed through questioning. The assessor will ask a minimum of **5 questions**, with follow-up questions where required.

The observation with questions is marked against the pass and distinction criteria included in the following pages.

- To achieve a **pass**, apprentices must achieve **all** of the pass criteria
- To achieve a **distinction**, apprentices must achieve **all** of the pass criteria and **all** of the distinction criteria
- **Unsuccessful** apprentices will have **not** achieved all of the pass criteria

Before the assessment

Employers/training providers should:

- ensure the apprentice knows the date, time and location of the assessment
- ensure the apprentice knows which professional security operative criteria will be assessed (outlined on the following pages)
- encourage the apprentice to reflect on their experience and learning on-programme to understand what is required to meet the standard and identify real-life examples
- be prepared to provide clarification to the apprentice, and signpost them to relevant parts of their on-programme experience as preparation for this assessment

Observation with questions mock assessment

It is the employer/training provider's responsibility to prepare apprentices for their end-point assessment. Highfield recommends that the apprentice experiences a mock observation with questions in advance of the end-point assessment with the training provider/employer giving feedback on any areas for improvement.

In designing a mock assessment, the employer/training provider should include the following elements in its planning:

- the mock interview should take place in a suitable location.
- a **2-hour** time slot should be available for the observation with questions, if it is intended to be a complete mock observation with questions covering all relevant standards (outlined in the following pages). However, this time may be split up to allow for progressive learning.
- consider a video or audio recording of the mock observation with questions and allow it to be available to other apprentices, especially if it is not practicable for the employer/training provider to carry out a separate mock observation with questions with each apprentice.
- ensure that the apprentice's performance is assessed by a competent trainer/assessor, and that feedback is shared with the apprentice to complete the learning experience. Mock assessment sheets are available to download from the Highfield Assessment website and may be used for this purpose.

- use a minimum of **5 structured 'open' questions** that do not lead the apprentice but allows them to give examples for how they have met each area in the standard. For example:

    - communicating with stakeholders
        - Describe a time you have effectively communicated with a stakeholder.
    - using various equipment while carrying out their duties
        - Outline the equipment you would use on a daily basis and how you would do this safely.
    - following instructions for security operations
        - Explain a time when you have successfully followed instructions for a security operation.
    - following procedures in the event of an incident
        - Explain the procedures you would follow in the event of an incident.
    - completing appropriate documentation
        - Give an example of documentation that has to be completed and what this entails.
    - operating control room equipment
        - Outline some of the control room equipment and what they are used for.
    - conducting searches
        - Describe a time you have successfully conducted a search and how this was done.

Observation with questions criteria

Throughout the **2-hour** observation with questions, the assessor will review the apprentice's competence in the criteria outlined below.

Apprentices should prepare for the observation with questions by considering how the criteria can be met.

Communication and customer service
To pass, the following must be evidenced.
CC1 Communicates respectfully with stakeholders using verbal and non-verbal means to establish a rapport and deliver customer service. (K12, K14, S7, S12, B4) **CC2** Acts responsibly to diffuse potential conflict situations by communicating in a calm and professional manner with others in a way that reflects the organisation's values. (S13, S15, B2, B5)
To gain a distinction, the following must be evidenced.
CC3 *Adapts their language and behaviour, in a calm and professional manner, in response to individual needs to exceed stakeholder expectations.* (K12, K14, S7, S12, B2)

Security operations
To pass, the following must be evidenced.
SO1 Navigates a site plan and assesses risk at the site or location by carrying out an observation of the designated area and reporting and recording any irregularities to the site risk assessment. (K26, S8, S9, S17) **SO2** Follows the assignment instructions and the clients or employers code of conduct and policies for behaviour, appearance, and the use of PPE. (S1, S11, B7) **SO3** Identifies and challenges suspicious activity across sites and locations, in line with SCaN principles, by being vigilant and aware of the area, and the movements and behaviours of people. (K9, K10, K25, S6, B1)
To gain a distinction, the following must be evidenced.
SO4 *Uses their knowledge of the site and usual movement and behaviour of people to recognise and check anomalies, showing awareness of the possible implications of these, reporting in line with procedures.* (K25, K26, S17, B1)

Security technology and equipment
To pass, the following must be evidenced.
ST1 In line with organisational procedures, uses security systems, applications, and technology to support security operations, and identifies faults with equipment taking remedial action where necessary. (K4, S3)
To gain a distinction, the following must be evidenced.
No distinction criteria

Security patrol, access, and searching – security control room operative pathway
To pass, the following must be evidenced.
SP1 Applies control room access control procedures to environments by carrying out searches and checking forms of authorisation, detecting and responding to unwanted activities. Reports findings in line with procedures. (K54, K57, K58, S34, S35, S36)
To gain a distinction, the following must be evidenced.
No distinction criteria

Security technology and equipment – security control room operative pathway
To pass, the following must be evidenced.
SE1 Operates the components of a control room system to gather and store images for evidential use, in line with organisational procedure. (K56, S38, S39)
To gain a distinction, the following must be evidenced.
No distinction criteria

Click here to return to contents

Assessing the professional discussion

The professional discussion will be a formal two-way conversation between the apprentice and assessor. It will give the apprentice the opportunity to make detailed and proactive contributions to affirm their competency against the criteria.

The apprentice must have access to their portfolio of evidence during the professional discussion. The apprentice can refer to and illustrate their answers with evidence from their portfolio of evidence (the portfolio of evidence is not directly assessed).

The professional discussion must take place in a suitable venue, for example, a quiet room, free from distractions and influence. It can be conducted by video conferencing.

The apprentice will have **2 weeks'** notice of the professional discussion.

The professional discussion must last for **60 minutes**. The assessor can increase the time by **10%** to allow the apprentice to respond to a question if necessary.

The assessor will ask a minimum of **8 questions**. Follow-up questions will be asked where clarification is required.

Employers will be allowed to be present during the assessment, however, in the interests of standardisation, they will **not** be permitted to ask questions or contribute to the assessment process. They may assist by allowing support in contextualising or using terminology that the apprentice better understands.

The professional discussion is marked against the pass and distinction criteria included in the following pages.

- To achieve a **pass**, apprentices must achieve **all** of the pass criteria
- To achieve a **distinction**, apprentices must achieve all of the pass criteria and **all** of the distinction criteria
- **Unsuccessful** apprentices will have **not** achieved all of the pass criteria

Before the assessment

Employers/training providers should:

- ensure the apprentice knows the date, time and location of the assessment
- ensure the apprentice knows which professional security operative criteria will be assessed (outlined on the following pages)
- encourage the apprentice to reflect on their experience and learning on-programme to understand what is required to meet the standard and identify real-life examples

- be prepared to provide clarification to the apprentice, and signpost them to relevant parts of their on-programme experience as preparation for this assessment

Professional discussion mock assessment

It is the employer/training provider's responsibility to prepare apprentices for their end-point assessment. Highfield recommends that the apprentice experiences a mock professional discussion in preparation for the real thing. The most appropriate form of mock professional discussion will depend on the apprentice's setting and the resources available at the time.

In designing a mock assessment, the employer/training provider should include the following elements in its planning:

- the mock professional discussion should take place in a suitable location.
- a **60-minute** time slot should be available to complete the professional discussion, if it is intended to be a complete professional discussion covering all relevant standards. However, this time may be split up to allow for progressive learning.
- consider a video or audio recording of the mock professional discussion and allow it to be available to other apprentices, especially if it is not practicable for the employer/training provider to carry out a separate mock assessment with each apprentice.
- ensure that the apprentice's performance is assessed by a competent trainer/assessor, and that feedback is shared with the apprentice to complete the learning experience. Mock assessment sheets are available to download from the Highfield Assessment website and may be used for this purpose.
- use a minimum of **8 structured 'open' questions** that do not lead the apprentice but allows them to express their knowledge and experience in a calm and comfortable manner. For example:
    - describe how your role in the team contributes to the organisation meeting its objectives.
    - explain the impact of an organisation not following industry regulations.
    - explain which digital communication systems you use to share information.
    - outline the methods you use for identifying prohibited items.
    - explain the ways you contribute to the improvement of processes to minimise security breaches.
    - describe a time that you have ensured public safety in a rapidly changing environment.

- describe an incident that required a barrier to be deployed.

Professional discussion criteria

Throughout the **60-minute** professional discussion, the assessor will review the apprentice's competence in the criteria outlined below.

Apprentices should prepare for the professional discussion by considering how the criteria can be met.

Legislation, regulation, and procedures
To pass, the following must be evidenced.
LR1 Describes how they apply industry regulation, legislation, guidance, and procedures in their role, acting with honesty and integrity, when monitoring risk and completing security documentation. (K1, K2, S2, S5, B9) **LR2** Explains how their role within the team, and their teams role within the organisation contributes to achieving the organisation's objectives, vision and values. (K5, K6) **LR3** Describes the range of internal and external factors that can affect performance of security systems and equipment, and how they have demonstrated a solutions focused approach in communicating ideas for improvement within the organisation. (K17, K28, B3)
To gain a distinction, the following must be evidenced.
LR4 *Analyses the potential impact of not following industry regulation, legislation, guidance, and procedures on security outcomes, including when monitoring risk and completing security documentation.* (K1, K2, S2, S5)

Communication and customer service
To pass, the following must be evidenced.
CC4 Explains how they use digital communication systems to record and share information for statutory and security purposes, in line with legislation and organisational procedure. (K15, S10) **CC5** Describes how they demonstrate a commitment to CPD, how they share this learning with others in a cooperative manner and how this can benefit the organisation. (B6, B8)
To gain a distinction, the following must be evidenced.
CC6 *Evaluates the importance of following guidance and procedures in the use of digital communication applications and information management systems and the possible impact on the individual, and organisation, if these are not followed.* (K15, S10)

Security incident response
To pass, the following must be evidenced.
SI1 Describes the methods for identifying weapons and other prohibited items, and how to apply these methods in line with organisation procedure. (K7) **SI2** Explains how they apply organisational procedures in the event of an incident or emergency, the actions they take in response and how they ensure the relevant people are engaged. (K8, S4)
To gain a distinction, the following must be evidenced.
SI3 *Justifies their response to an incident or emergency, and how they ensured public safety in rapidly changing circumstances.* (K8, S4)

Security operations
To pass, the following must be evidenced.
SO5 Explains how they contribute to the review and improvement of processes and procedures to support organisational improvement and how these reviews minimise the risk of reputational damage by improving the removal of certain items, objects or behaviours in particular areas. (K24, S14) **SO6** Explains how allowing some behaviours or items in certain areas can have a negative impact on the organisations reputation, why this is important, and how they contribute to improving processes and procedures. (K3, K24, S14)
To gain a distinction, the following must be evidenced.
No distinction criteria

Security incident response – security control room operative pathway
To pass, the following must be evidenced.
SR1 Describes incidents that have required a barrier to be deployed, how they determined the correct type of barrier and how they ensured it was deployed correctly and in line with organisational procedures. (S37)
To gain a distinction, the following must be evidenced.
No distinction criteria

Click here to return to contents