

Highfield Level 3 End-Point Assessment for ST0189 Fire, Emergency and Security Systems Technician

End-Point Assessment Kit



Highfield Level 3 End-Point Assessment for ST0189 Fire, Emergency and Security Systems Technician

EPA Kit

Contents

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

Introduction	5
The Highfield approach	9
Gateway	10
The Fire, Emergency and Security Systems Technician apprenticeship standard	12
Assessment summary	51
Assessing the multiple-choice test	54
Assessing the practical assessment with questioning	56
Assessing the interview underpinned by a portfolio of evidence	64

How to use this EPA Kit

Welcome to the Highfield End-Point Assessment Kit for the Fire, Emergency and Security Systems Technician 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 3 Fire, Emergency and Security Systems Technician 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.

Key facts

Apprenticeship standard:	Fire, Emergency and Security Systems Technician
Level:	3
On-programme duration:	Typically 36 months
End-point assessment window:	3 months
Grading:	Pass/distinction
End-point assessment methods:	Multiple-choice test Practical assessment with questioning Interview underpinned by a portfolio of evidence

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 fire, emergency and security systems technician is responsible for the planning, installation, testing, commissioning and handover of fire, or security systems equipment. The broad purpose of this occupation is to protect individuals, homes and properties from risk and danger. To do this they use a wide range of systems and various communication technologies with electrical and electronic components.

Key responsibilities are likely to include installing systems, conducting preventative and corrective maintenance, and diagnosis of faults and repairing these on systems and their components. Technicians will initiate own and complete processes, tasks and procedures, supporting the wider team to deliver security and safety services.

Typical job titles may include alarm installer, alarm technician, fire systems engineer, fire systems installer, security systems engineer and security systems installer.

This standard aligns with the Institute of Engineering and Technology for Engineering Technician (EngTech) professional recognition. Upon completion, apprentices may choose to act on this.

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 Fire, Emergency and Security Systems Technician 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 interview and collation of the portfolio of evidence (such as a provision of recordings of professional discussions or workplace evidence).

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 2 English and maths
- any qualifications specified by the employer
- completion of a portfolio through which the apprentice gathers evidence of their progress

- 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

Throughout the period of learning and development, and at least every **2 months**, the apprentice should meet with the on-programme assessor to record their progress against the standard. At these reviews, evidence should be discussed and recorded by the apprentice. The maintenance of an on-programme record is important to support the apprentice, on-programme assessor and employer in monitoring the progress of learning and development. This will determine when the apprentice has achieved full competence in their job role and is therefore ready for end-point assessment.

Portfolio of evidence

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 interview underpinned by a portfolio of evidence.

It will typically contain **5 discrete pieces of evidence**. Evidence may be used to demonstrate more than **1 knowledge, skill or behaviour** as a qualitative approach is suggested as opposed to a quantitative approach.

Evidence sources for the portfolio may include:

- workplace documentation and records
- workplace policies and procedures
- witness statements
- annotated photographs
- video clips with a maximum total duration of 10 minutes and where the apprentice must be in view and identifiable

This is not a definitive list and other evidence sources are possible. Given the breadth of context and roles in which this occupation works, the apprentice will select the most appropriate evidence based on the context of their practice against the relevant knowledge, skills and behaviours.

The portfolio should not include reflective accounts or any methods of self-assessment. Any employer contributions should focus on direct observation of performance (for example, witness statements) rather than opinions.

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 interview.

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 on-programme requirement - apprentices must hold an Electrotechnical Certification Scheme (ECS) card. This will allow apprentices to progress to the end-point assessment gateway.

Readiness for end-point assessment

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

- the apprentice must have achieved **Level 2** English and maths.
- the apprentice must hold an Electrotechnical Certification Scheme (ECS) card.
- the apprentice must have gathered a **portfolio of evidence** against the required elements to be used as the basis for the interview.
- 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.
 - Health and safety
 - Security and fire risk assessments
 - Maintenance and repairs
 - Sustainability
 - Data collection and storage
 - Equality and diversity

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.

Order of end-point assessments

There is no stipulated order of assessment methods. 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

Standard (2023)

<https://www.instituteforapprenticeships.org/apprenticeship-standards/fire-emergency-and-security-systems-technician-v1-1>

End-point assessment plan (ST0189/v1.1)

<https://www.instituteforapprenticeships.org/apprenticeship-standards/fire-emergency-and-security-systems-technician-v1-1>

Specific considerations

Highfield has mapped the practical assessment with questioning criteria to the specific tasks that the apprentice will complete in the assessment.

[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:

- achieved **Level 2** English
- achieved **Level 2** maths
- compiled a portfolio of evidence
- gained an Electrotechnical Certification Scheme (ECS) card
- submitted their organisation's policies and procedures as requested by Highfield

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](#)

The Fire, Emergency and Security Systems Technician 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.

Multiple-choice test

K1 Awareness of **Health and safety legislations, codes of practice and safe working practices**, relevant to the occupation and the operative's responsibilities. Including Health and Safety at Work Act, BS 7671, BS EN 50131, BS EN 62676 and BS 5839.

K2 **Testing techniques for electrical and electronic components used in fire detection and alarm systems. The principles of using meters, applying Ohms law, formulae, calculations and taking readings.**

K3 The principles of **fire detection and fire alarm systems: features and design criteria, survey methods** and impact on the fire safety industry.

K7 Principles of **planning and project management** of fire and security **system installation: commissioning, and handover.**

K8 **Data collection, storage and sharing methods and techniques.**

K12 **Principles and techniques for installing and maintaining electronic systems: SI units, quantities, formulae and calculations, electromagnetism and electromagnetic induction, ICT applications, smart Apps and power supplies.**

K15 **Testing techniques for electrical and electronic components used in intrusion alarms, access control systems and video surveillance systems (CCTV). The principles of using meters, applying Ohms Law, formulae, calculations and taking readings.**

K17 Techniques for **planning and installing systems cabling; methods of containment and protection.**

K19 **The principles of intrusion alarms, access control, video surveillance (CCTV) features and design criteria, survey methods** and impact on the building security industry.

Amplification and guidance

- **Health and safety legislations, regulations and procedures:**
 - legislations and regulations may include:
 - Health and Safety at Work Act etc. – legislation covering occupational health and safety in the UK
 - Work at Height Regulations – applies to all work at height where there is a risk of injury from falling and falling objects
 - Workplace (Health, Safety and Welfare) Regulations – to provide facilities that improve the health, well-being and safety of employees
 - Control of Noise at Work Regulations – requires employers to prevent or reduce risks to health and safety from exposure to noise at work, including action values and limit values, requires hearing protection to be used when noise exposure reaches and exceeds 85 dBA
 - Construction Design and Management Regulations – ensures health and safety issues are appropriately considered during the development of construction projects
 - Electricity at Work Regulations – isolation of from all sources of electricity before starting work on electrical systems
 - Control of Substances Hazardous to Health Regulations (COSHH) – assess, prevent and control exposure to substances and provide information, instruction and training
 - procedures may include:
 - Appropriate Personal Protective Equipment (PPE) – wearing the suitable workwear such as eye protection, ear defenders and gloves
 - Health and Safety Executive (HSE) guidelines – providing guidance, regulations and rules on workplace health and safety
 - Risk Assessment and Method Statement (RAMS) – recording the risks associated with a job and detailing how these will be managed
- **Codes of practice** including:
 - National Security inspectorate (NSI)
 - British Security Industry Association (BSIA)
 - British Standards Institution (BSI) – provide codes of practice for the industry. Some of these are:
 - BS 7671 (wiring/cables)
 - BS EN 50131 (intruder alarms)
 - BS EN 62676 (video surveillance systems)
 - BS 5839 (fire)
- **Safe working practices** include:
 - the safe handling of situations and materials
 - following working at height processes

- keeping up with housekeeping (reducing of slips and trips)
 - ensuring the isolation of electrical supplies before starting work on electrical systems
 - completing risk assessments to identify hazards and minimise them/completing a RAMS document
 - voltage indicators that are used in the safe isolation procedure complying with HSE GS38
 - following the internal and industry codes of practice
 - following Safe Systems of Work (SSOW) procedures
 - using the appropriate PPE for the situation and environment, such as to control the exposure to hazardous substances
 - having the adequate training to use equipment, and providing health and safety site inductions
 - holding a permit to work – this enables certain jobs to be carried out safely under controlled conditions
 - using tools and equipment on site safely such as an insulation test meter, and ensuring the correct voltage of power tools, cabling and metal
- **Testing techniques for electrical and electronic components used in fire detection and alarm systems:**
 - a continuity test is conducted to assess battery life
 - insulation resistance testing is performed to verify adequate insulation
 - a voltage drop at the end of a circuit can be caused by excessive resistance in the circuit
 - according to BS5839-1 the standby time and alarm load are factors to consider when calculating the battery capacity required for a fire alarm system
 - when a metre reads infinite resistance it indicates an open circuit
 - an ammeter reading zero indicates an open circuit
- **The principles of using meters** may include:
 - accurately taking and interpreting readings, ensuring appropriate range settings on meters are being used
 - ensuring safety checks are carried out before use, taking note of any defects or damage
 - awareness of the importance of calibration of meters to ensure accurate readings
 - utilising specialised meters, such as clamp meters for alternative current measurements
- **Applying Ohms law:**
 - implement Ohm's Law ($V=IR$) to determine the relationship between voltage (V), current (I) and resistance (R)
 - this principle is used to diagnose circuit issues and component performance

- **Formulae and calculations:**
 - apply formulae for calculating power ($P=VI$)
 - calculate total resistance in series and parallel circuits:
 - for resistors in a series, the total resistance (R_{total}) is the total of all resistances: $R_{total}=R_1+R_2+R_3+...$
 - in parallel, the total resistance (R_{total}) is calculated by the following calculation: $1/R_{total}=1/R_1+1/R_2+1/R_3+...$

- **Taking readings** may include:
 - using multimeters to measure voltage at various points of the installation
 - using multimeters to measure resistance at various points of the installation
 - using multimeters to measure current at various points of the installation
 - being able to determine if readings obtained are within expected parameters
 - documenting readings for troubleshooting and validation

- **Fire detection systems features and design criteria:**
 - the main function of a fire detection system is to alert people that there is a fire
 - fire alarm systems should be maintained by a responsible person
 - the main types of smoke detectors include:
 - ionisation
 - photoelectric
 - a combination of ionisation and photoelectric
 - a smoke detection system detects fires early
 - automatic fire detectors (AFD) are able to detect the earliest signs of fire and alert the building's occupants without human intervention
 - to minimise unwanted alarms a manual call point is fitted with a plastic cover
 - the minimum cable conductor size for fire alarm detection wiring is 1mm
 - the sensing element of heat detectors is commonly known as the thermistor
 - flame detectors use thermal imaging to detect fires
 - the main types of flame detectors include:
 - ultraviolet
 - infrared
 - ultraviolet and infrared

- multi-spectrum infrared
- visual flame imaging
- **Fire alarm systems features and design criteria:**
 - the main types of fire alarm systems include:
 - conventional
 - addressable
 - wireless
 - analogue
 - fire alarm systems range from grade A through to F (Grade B and E systems are no longer recognised). Commercial systems often fit into one of the following categories:
 - category M (systems are 'M' if they are manual systems)
 - category L1 (systems are 'L' if they are designed to protect life)
 - category L2
 - category L3
 - category L4
 - category L5
 - category P1 (systems are 'P' if they are designed to protect property)
 - category P2
 - in buildings manual call points are typically sited at escape routes and exits.
 - no one should have to travel more than 45 metres to access a call point, unless the route is undefined then the maximum travel distance is 30 metres.
 - category L1 systems must be installed throughout all areas of the building.
 - category M systems are installed in buildings where occupants are likely to notice a fire.
 - at a minimum, 25% of monitored fire alarm systems must be tested quarterly.
 - a fire alarm control panel integrates with an access control panel with an access control door entry system via a changeover relay.
 - monitored system maintenance visits must not exceed 6 months, with 100% of devices tested within the 12-month period.
 - BS 5839-6:2019+A1:2020 covers all domestic properties.

- **Survey methods** may include:
 - risk assessment survey
 - site survey
 - maintenance and testing survey
 - compliance audit survey
 - site modification survey
 - survey requirements are:
 - existing systems should be evaluated during a survey to assess the compatibility of new additions
 - the first step in designing a new system should be conducting a site survey
 - the process of upgrading an existing system to meet current safety standards is known as 'retrofitting'

- **Planning and project management:**
 - within the project planning phase a timeline should be established, and resources be allocated
 - milestones and deadlines should be included in the project timeline
 - project scope refers to what the project aims to achieve
 - zone charts can be used to identify areas of detection
 - organisational and Gantt charts can be used
 - unforeseen circumstances should be considered, which includes things such as bad weather and data breaches
 - the project manager is responsible
 - within the planning stage, user requirements can be identified by communicating with them about what the system is intended for
 - the project schedule should consider the requirements of the stakeholders
 - during the final stage of the project, a handover checklist should be completed
 - the final acceptance test during the handover of the project is completed by an independent third-party certifier

- **System installation:**
 - before installing a system, a site survey should have been carried out
 - wireless technology can be used
 - alarm transmission and aspirating systems
 - fire systems:
 - the installation of cables, conduits and back boxes is typically referred to as a 'first fix'

- a low smoke fume (LFS) cable should be used for fire alarm installations
 - fire alarm zone charts can be devised to demonstrate specific areas of the building where exits and common escape routes are
- security systems:
 - door entry panels and readers must be installed at different heights to comply with the Equality Act
 - on new installations when the system is activated, the audible side of an external warning device should operate for 15 minutes
 - following the Building Regulation Approved Document B
- **Commissioning:**
 - the commissioning stage is focused around ensuring that the system functions as designed.
 - the commissioning process must be carried out by a competent person. This is someone who has the necessary skills, knowledge and experience.
 - integrated systems testing can contribute to the commissioning process by evaluating the overall efficiency of systems in various scenarios.
 - commissioning should be completed after the system is installed.
- **Handover:**
 - effective communication is essential with all stakeholders within this stage
 - a customer must understand how to locate a detection device installed on the system
 - the engineer should provide the customer with a complete circuit list of device locations with a marked drawing
 - once handover has been completed, the system should be maintained in line with its requirements
- **Data collection:**
 - data may be obtained at multiple points during a customer's journey. Any information obtained must not be excessive and must align with General Data Protection Regulations (GDPR).
 - two-factor authentication is the most secure method of data retrieval
 - data is often collected through:
 - industry specific surveys – surveys and questionnaires may be requested to be completed by customers and clients. The data collected must be in line with GDPR.
- **Data storage techniques:**
 - security industry databases:

- establishing robust databases with strong encryption protocols to ensure the confidentiality and integrity of sensitive data, including client information and system specifications
 - cloud solutions:
 - cloud storage solutions that comply with industry-specific security standards, ensuring data is accessible yet protected against unauthorised access
 - the process of changing digital data in a storage device is known as manipulating
- **Data sharing methods:**
 - When sharing data there must be strict adherence to industry-specific regulations and standards, such as GDPR to ensure ethical and legal Data-sharing practices
 - .zip files are used to compress files for easier transfer
 - Bandwidth describes the amount of digital data that is transmitted between devices over a network
 - Mesh topology
 - RS485 can be used to transmit data over long distances in access control systems
 - Encrypted communication:
 - robust methods must be implemented for data transmission to ensure that sensitive information remains secure during sharing with stakeholders
- **Principles and techniques for installing and maintaining electronic systems:**
 - the main function of power supplies in fire and security systems is to convert AC to DC
 - a fuse is used to prevent overcurrent by breaking the circuit
 - smart apps in security systems typically communicate with users through the internet
 - a rectifier is essential for converting Ac to DC in electronic systems
 - a wattmeter is used to measure electrical power
 - when selecting a power supply the voltage and current requirements of the system should be the main consideration
 - twisted pair cabling can be used in the installation of data cabling to reduce signal interference
- **SI units and quantities:**
 - correct use of SI units such as volts (V) for voltage, amperes (A) for current and ohms (Ω) for resistance
 - understanding key quantities such as electrical charge (Coulombs), energy (Joules), power (Watts) and magnetic flux density (Tesla)

- awareness of prefixes and factors for the base units from largest to smallest factor: kilo, hector, deca, base unit, deci, centi and milli
- **Formulae and calculations:**
 - calculation and application of Ohm's Law ($V=IR$)
 - calculations involving energy consumption and power ratings
 - use of formula and calculations to determine resistance, capacitance in parallel and series
- **Electromagnetism fundamentals:**
 - exploration of magnetic fields around conductors and coils, and their practical implications in electronic design
 - understanding the force exerted by magnetic fields on electrical circuits
- **Electromagnetic induction:**
 - principles of inducing voltage in a conductor through a changing magnetic field
 - applications in transformers, inductors and electromagnetic compatibility considerations
- **ICT applications:**
 - understand basic IP networking concepts, crucial for configuring and managing fire and security systems
 - utilise subnets to organise network devices efficiently, enhancing security and performance
 - employ port forwarding to facilitate remote access to specific devices within the network
 - leverage software tools for precise system configuration, ensuring optimal operation
 - assign a unique IP address to each IP camera when configuring it to ensure recognisable network communication
 - implement remote support solutions to diagnose and resolve issues swiftly, minimising system downtime
 - understand network protocols and standards to ensure secure and reliable data communication within fire and security systems
- **Smart apps** can be used for:
 - real-time alerts and system status monitoring
 - maintenance scheduling and incident reporting
 - job tracking, documentation and communication
 - real-time communication among team members

- **Power supply technologies:**
 - comparison of AC vs DC power systems and their suitability for various applications
 - overview of battery technologies, solar power and other renewable energy sources for electronic systems

- **Testing techniques for electrical and electronic components used in intrusion alarms, access control systems and video surveillance systems (CCTV):**
 - voltage: confirm equipment operates correctly across conditions, within manufacturer specifications
 - current: check operation considering current consumption and system functionality without mains power, if applicable
 - battery systems: test for adequate charging, output voltage and capacity according to specifications
 - techniques for testing specific systems:
 - CCTV: check digital video recorder (DVR) and network video recorder (NVR) functionality including playback and features like motion detection (assess video quality under all conditions)
 - Intruder systems: test system operations including arming/disarming
 - Access control: verify system operations like lock/unlock, emergency egress and features such as roll call
 - Signalling: confirm timely communication of alarms and conditions to appropriate recipients
 - Wireless: analyse wireless signal strength to ensure stable device communication
 - fault finding and diagnosis:
 - visual inspection: identify any damage needing immediate attention
 - system analysis: use diagnostic tools and system logs to pinpoint issues
 - error review: examine error codes and logs for patterns indicating problems
 - stress testing: ensure reliability under various conditions
 - the current drawn by an electronic lock can be measured using an ammeter in series with the lock
 - in an intruder alarm system the term 'end of line' refers to the resistance at the last device in the circuit
 - anti-passback configuration testing prevents unauthorised re-entry
 - when testing the voltage on an intruder alarm passive infrared (PIR) a multimeter should be set to 20V
 - capacitors in power supplies are used to smooth out voltage fluctuations
 - increasing the diameter of the conductor can reduce significant voltage drops in a circuit
 - obtaining charging voltage readings is important to ensure the batteries are charging at the required voltage

- **Planning and installing systems cabling:**
 - adherence to BS7671 ensuring all cabling practices comply with BS7671 regulations for electrical installations
 - use of detailed plans and drawings to identify existing cabling routes and plan new installations, minimising disruptions and ensuring optimal cable routing
 - secure cables to the building's structure at suitable intervals to prevent premature collapse, especially in fire conditions, enhancing system resilience
 - during and/or after the installation, produce as-wired drawings that accurately reflect the installed cabling routes and types
 - provide all necessary documentation, including as-wired drawings and plans, to support future system maintenance, expansions and fault finding
 - ensure necessary earthing of metal containment systems and all mains carrying conductors to ensure electrical safety and compliance with regulatory standards
 - ensure electrical and communication cables are separated to prevent signal interference
 - use of cable catenary systems to provide structural support for cable runs
 - follow the bending radius guidance when installing cabling to prevent damage to the conductors

- **Cabling selection:**
 - consider the specific needs of the system, whether it's for data transmission, power supply or security applications, to determine the appropriate cable type.
 - select cables that are suitable for the environment they will be installed in, considering factors like moisture, temperature and potential mechanical stresses. Such as shielded cables should be used if the environment is subject to electrical noise.
 - maintain strict adherence to local and national building codes, alongside BS7671, to ensure the safety and reliability of the cabling infrastructure.
 - cables connecting the final low voltage mains supply to a fire alarm must be fire resistant.
 - a linear heat detection cable provides detection for the entire length of the cable.

- **Methods of containment and protection:**
 - utilise cable trays, conduits and trunking to protect cables from physical damage and to maintain an organised cabling infrastructure.
 - adherence to fire-stopping measures and prevention of compromising the compartmentation to prevent the spread of fire and smoke, maintaining the integrity of cabling routes.

- provide mechanical protection in areas prone to damage, ensuring cable integrity. This may include the use of containment or cables which contain mechanical protection, such as armoured cables.
- containment can be used to enhance shielding from electromagnetic interference such as galvanised conduit.
- **The principles of intrusion alarms, access control, video surveillance (CCTV)**
 - A passive infrared (PIR) and microwave (radar doppler effect) are commonly combined to make up a dual-tech sensor
 - 2 PIRs cannot be sited where the range of coverage would overlap
 - According to BS 5839, manual call points must be mounted at 1.4m (+/-300mm)
 - GPRS is commonly used by monitored signalling devices
 - In the UK, the standard operating mains frequency for CCTV is 50 Hz
 - The confirmation window between the first detection zone activating and the second detection zone activating that triggers a confirmed alarm condition is 30 to 60 minutes
 - According to BS 9263 grade 1 intruder and hold-up alarm systems only require 1 site visit service per year
 - If a hold-up alarm system requires sequential verification the time window between triggering the first and the second alarm will be 8 to 20 hours
 - BS EN 60839-11-2 outlines the application guidelines for access control systems
 - The maximum permitted entry time varies between systems, such as for Grade 3 systems it is 45 seconds
 - The back-up battery should sustain a Grade 3 intruder alarm system if the alarm receiving centre is notified of a mains failure for 12 hours
 - Power over Ethernet cameras have the ability to receive both power and data through a single ethernet cable
 - A pan tilt zoom camera is used to cover a large area or to follow movement
 - The standby battery time for a Grade 3 and Grade 4 system can be reduced to 12 hours from 24 hours if the system signals 'mains fail' to the Alarm Receiving Centre (ARC)
 - BS EN 50131 states that:
 - motion sensors must have anti-masking features for grade 3 and above systems
 - the tamper detection of grade 2 wire-free systems should be opened by normal means and removed from the mount
 - it is recommended that a class IV detector is installed outdoors
- The **design criteria** of systems. The design of a system must:
 - be scalable and adaptable, which meets the building's changing security needs, considering future modifications

- align with the grading as stated by the security risk assessment or as instructed by the insurance company
 - take into account the environmental classification of equipment to match the environmental requirements of the system
 - consider the ease of use, ensuring that security personnel can efficiently operate and manage the systems
 - consider the effects of environmental elements like dust, humidity and extreme temperatures on its components and design accordingly
 - ensure that CCTV systems are positioned to provide clear visibility under various lighting conditions
 - consider easy access to all components for future maintenance, minimising downtime and ensuring system reliability
 - implement measures to prevent false alarms, which can undermine security effectiveness and waste resources
- To determine the required system, **features and design criteria** risk assessments are completed. These:
 - are completed through conducting thorough surveys to assess and identify potential security risks within and around the building to determine a grade of the system. These include:
 - grade 1 intruder alarms – low level of risk
 - grade 2 intruder alarms – low to medium level of risk (a 2e system is audible only)
 - grade 3 intruder alarms – medium to high level of risk
 - grade 4 intruder alarms – high level of risk
 - evaluate environmental factors such as lighting, weather and local activities that could impact system performance.
 - evaluate environmental classification of intruder components to ensure correct operation of equipment. These classifications are:
 - Class I – indoor: indoor environments that have a well maintained temperature, such as residential properties
 - Class II – indoor – general: indoor areas with less-controlled temperatures, such as corridors and halls
 - Class III – outdoor – sheltered or indoor extreme conditions: outdoor spaces with partial exposure to weather or extreme indoor conditions
 - Class IV – outdoor – general: outdoor areas with full exposure to weather

Health and safety	
Skills	Behaviours
S1 Comply with safety legislation , codes of practice, risk assessments , method statements , safe systems of work and apply control measures .	B1 Puts workplace health, safety and wellbeing first for self and others.
Practical assessment with questioning	
Pass criteria	
<p>HS1 Prioritises workplace health, safety and wellbeing and complies with health and safety regulations, standards and guidance in line with the task requirements (S1, B1)</p>	
Amplification and guidance	
<ul style="list-style-type: none"> • Comply with safety legislation by: <ul style="list-style-type: none"> ○ regularly cleaning and organising the workspace to remove potential tripping hazards, clutter and debris ○ storing tools, equipment and materials in designated areas to prevent accidents and maintain clear pathways ○ routinely inspecting and maintaining equipment to ensure safe operation and promptly address any defects or hazards ○ immediately reporting any unsafe conditions, incidents or near-misses to supervisors or relevant authorities ○ ensuring clear communication with team members about safety procedures and changes in the work environment to promote a collective commitment to safety ○ maintaining records of safety-related activities, including hazard reports, safety meetings and training records ○ wearing the appropriate personal protective equipment (PPE) as indicated in risk assessments and safe systems of work, such as helmets, safety glasses, gloves and safety shoes ○ regularly inspecting and maintaining personal protective equipment to guarantee its effectiveness and integrity 	

- **Risk assessments and method statements:**
 - should be conducted to identify all potential hazards and understand the sequence of tasks and safety measures
 - seek clarification on any unclear aspects of risk assessments or method statements from supervisors or safety experts to ensure complete comprehension
 - execute safe systems of work meticulously, adhering to each step and guideline to minimise risks during tasks
 - attend regular training sessions to stay updated on safety procedures and the appropriate execution of tasks

- **Apply control measures:**
 - apply control measures precisely as specified in risk assessments to prevent accidents and protect individuals involved in the work
 - maintain vigilance and continuously assess the work environment for any unexpected hazards or changes that may require adjustments to control measures
 - be prepared to respond swiftly and effectively in the event of an emergency, ensuring the safety of oneself and others

- **Put workplace health, safety and wellbeing first by:**
 - following health and safety guidelines and legislation
 - taking responsibility for own safety and for those around
 - keeping a tidy and safe work environment
 - identifying potential hazards by completing risk assessments
 - wearing the correct personal protective equipment (PPE)
 - employing good housekeeping practices and waste management procedures

Diagnostics and fault finding

Skills

S4 Carry out takeover procedure, diagnose and repair faults.

Practical assessment with questioning

Pass criteria

DF1 Carries out takeover procedures and applies diagnostics techniques prior to repairing faults in line with the task requirements and manufacturer's instructions (S4)

Amplification and guidance

- **Carry out takeover procedure, diagnose and repair faults:**
 - ensure that the correct electrical readings are taken, including voltage, current and resistance readings
 - ensure that company documentation has been completed accurately and in detail
 - identify and document non-compliances during takeover
 - ensure that all faults are documented accurately

- **Diagnose faults:**
 - ensure that the fault is correctly diagnosed
 - ensure correct equipment is selected to rectify the faults
 - ensure the correct use of equipment to diagnose faults, including:
 - Multimeters
 - Scopes
 - Loop testers

- Test monitors
- Hochiki programmer
- Testifire smoke/heat tester

Risk assessments	
Knowledge	Skills
K5 Principles of security and fire risk assessments: function, content and how to implement them.	S8 Carries out risk assessments.
Practical assessment with questioning	
Pass criteria	
RA1 Carries out risk assessments in line with the task requirements, organisational procedures and legal and regulatory requirements (K5, S8)	
Amplification and guidance	
<ul style="list-style-type: none"> • Risk assessments: function, content and how to implement them: <ul style="list-style-type: none"> ○ they are carried out to identify vulnerabilities and threats so that they can be minimised ○ a risk assessment should be carried out before the job is started – the results should be received by the installer ○ they are influenced by complexity, size of the property and risk level ○ a risk assessment determines the relevant grade/category of system that will be required • Carries out risk assessments: <ul style="list-style-type: none"> ○ ensure that the relevant information is attained to establish the system grade ○ ensure an understanding of the requirements of the relevant British Standards and relevant industry codes of practice 	

- identify hazards and how to mitigate them
- have a full understanding of the ABC (area, boundary and contents) of risk
- carry out a dynamic risk assessment during installations
- ensure that the kit selected meets the grade of the system (grade 1-4)

Commissioning, testing and handover

Knowledge	Skills	Behaviours
K18 The use of digital information systems in the fire and security safety sector.	<p>S2 Complete functionality tests of systems and components during commissioning systems.</p> <p>S5 Operate ICT equipment and systems to store, retrieve, manipulate, transmit or receive digital data and electronic information.</p> <p>S7 Complete functionality tests of systems and components during handover of systems.</p>	B5 Acts ethically.
Practical assessment with questioning		
Pass criteria		
<p>CT1 Completes functionality tests of systems and components during commissioning and handover in line with the task requirements and manufacturer’s instructions (S2, S7)</p> <p>CT2 Uses digital information systems to store, retrieve, manipulate, transmit and receive digital data and electronic information in line with the task requirements following legal and regulatory guidance, GDPR and ethical principles (K18, S5, B5)</p>		

Amplification and guidance

- **Digital information systems:**
 - digital equipment that technicians use:
 - PC or laptop for programming fire and security systems
 - PC or laptop for remote maintenance and support
 - PDA or mobile for sending and receiving jobs
 - units of measurement:
 - frames per second
 - file sizes such as bytes, megabytes, gigabytes and terabytes
 - formulae to calculate storage capacity to meet the operational requirement of the system
 - formulae to calculate battery calculations
 - data security:
 - ensure that data is adequately protected
 - use secure passwords, data encryption methods and anti-virus software
 - understand firewall rules and port forwarding

- **Complete functionality tests of systems during commissioning:**
 - ensure that the correct electrical readings are taken, which include voltage, current and resistance readings
 - complete any company documentation accurately and in a detailed manner, including:
 - completing company adopted documentation
 - accurately recording non-compliances on commissioning documentation
 - documenting all faults accurately
 - completing commissioning documentation recording readings and tests
 - ensure that systems are fully tested by:
 - completing tests on 100% of equipment
 - completing test voltages of batteries and power supplies

- measuring resistance of cables
- completing walk tests of the system
- testing for volt drop
- completing insulation resistance tests
- completing tests of earthing
- systems are tested to ensure that they are compliant with the necessary standards. These are:
 - BS 9263
 - BS 5839
 - BE EN 50131
 - BS 8243
 - PD 6662
 - BS EN 62676
 - BS EN 60839
- **Operate ICT equipment and systems:**
 - Emailing systems to communicate with staff and clients
 - Instant messaging apps to communicate
 - Database software for storing client data
 - Word processing software
 - PDF viewers for reading manufacturer's information and manuals
 - Customer relationship management (CRM) software for client data storage
 - Software to upload and download information, and documents for remote support and maintenance
- **Store digital data and electronic information using:**
 - Physical hard drives
 - DVDs

- Network attached storage (NAS Drive)
- Cloud storage
- CD-ROM's
- External hard drives
- Solid state hard drives
- USB flash drives

- **Transmit or receive digital data and electronic information:**
 - methods of data transmission such as RS485, RS232 and VOIP
 - serial transmission between USB/COM port on laptop and panel
 - wireless transmission using internet, point-to-point communication
 - relabel zones and devices on the panel correctly
 - change the engineer code

- **Complete functionality tests during handover:**
 - ensure that a full demonstration of the system is carried out to the user
 - recommend that the end user documents the demonstration
 - ensure that the system meets the specified operational requirements and needs of the client
 - ensure that the relevant signage is displayed to meet legislation requirements (for CCTV there is no signage available in FESS bays)
 - ensure handover documentation is completed
 - ensure that the 'As Fitted' documentation is completed accurately

- **Act ethically by:**
 - maintaining customer confidentiality
 - keeping customer data and information secure
 - being sensitive and considerate to different cultures, types of customers and their needs

- being honest and transparent with customers and colleagues
- ensuring that activities and systems conform to safety standards
- not sharing engineer codes with the public

Installation

Skills

S3 Apply and implement system design, planning and installations including additional components to existing systems.

S12 Plan and install systems cabling.

Practical assessment with questioning

Pass criteria

IN1 Plans and installs systems cabling, in line with the task requirements, manufacturer's instructions and legal and regulatory requirements (S12)

IN2 Applies and implements system design, in line with the task requirements, manufacturer's instructions and legal and regulatory requirements (S3)

Amplification and guidance

- **Apply and implement system design, planning and installations:**
 - risk assessments:
 - ensure the building has been risk assessed to identify the grade of the system to be installed
 - ensure the risk assessment is correct and up to date, as the use of the building may have changed since the original installation
 - identify risks and mitigate them
 - understanding documentation and plans:
 - read and understand existing system design proposals, building layout drawings and system schematics

- costs:
 - ensure that the additions are cost effective and meet the level of risk
 - ensure that customers are not paying for unnecessary equipment
 - ensure that all equipment is included so that the company does not operate at a loss

- **Additional components to existing systems:**
 - ensure current and new system components are compatible with the existing system
 - locate existing expansion modules and components on an existing system
 - decide where the best position is to install additional components
 - seek clarification from the customer on how the system is operated so points of entry and exit can be identified

- **Plan systems cabling:**
 - plan cable routes accordingly, away from high-voltage services and consider what needs to be done to cross a high-voltage cable
 - identify routes to minimise waste cable
 - identify various types of containment for cabling
 - consider the location and environment to ensure that the suitable cable is selected
 - consider segregation from other services to avoid interference
 - consider cable distance and any limitation factors
 - consider the wiring topology required, as different systems require different types of wiring

- **Install systems cabling:**
 - ensure that the cable installed is compliant with the relevant standard for the required task
 - ensure that the cable is suitably fixed to the surface
 - ensure that fixings are compliant with industry standards, such as BS7671
 - ensure that the cables are mechanically protected with suitable containment where required
 - ensure the cable size meets the requirements of the job

- ensure spare capacity of cable where required
- consult with other standards, such as BS7671 and BS5839
- ensure the type of cabling is suitable for the job, for example, screened cabling may be required for certain types of data bus

System maintenance	
Knowledge	Skills
K4 Principles and techniques for maintaining fire detection and alarm systems and their components using tests, diagnostics, taking readings and recording information.	S13 Carry out maintenance activities on fire detection and alarm systems and their components.
K6 Principles and techniques for maintaining intrusion alarm, access control, video surveillance (CCTV) and their components using tests, diagnostics, taking readings and recording information.	S14 Carry out maintenance activities on intrusion alarm, access control, video surveillance (CCTV) and their components.
Interview underpinned by a portfolio of evidence	
Pass criteria	<i>Distinction criteria</i>
SM1 Describes how they carry out maintenance activities on fire detection and alarm systems and their components in line with manufacturer's guidance, organisational procedures and legislative regulations and guidance (K4, S13)	SM3 <i>Explains the importance to the customer and the organisation of following manufacturer's guidance, organisational procedures and legislative regulations and guidance when maintaining fire detection and fire safety systems and components (K4, S13)</i>
SM2 Describes how they carry out maintenance activities on intrusion alarm, access control, video surveillance (CCTV) and their components in line with manufacturer's guidance, organisational procedures and legislative regulations and guidance (K6, S14)	SM4 <i>Explains the importance to the customer and organisation of following manufacturer's guidance, organisational procedures and legislative regulations and guidance when maintaining intrusion alarm, access control, video surveillance (CCTV) and their components (K6, S14)</i>

Amplification and guidance

- **Principles and techniques for maintaining fire detection and alarm systems:**
 - understanding system fundamentals:
 - know the various components like detectors, panels and alarms, and understand their roles within the system
 - understand how the system activates in response to fire signals
 - maintenance:
 - understand the difference between routine maintenance (to prevent faults) and corrective maintenance (actions taken after system failures)
 - understand the importance of system reliability and how maintenance impacts it
 - safety standards and regulations:
 - be aware of regulations surrounding maintenance, as indicated in BS5839-1, which dictate preventative maintenance frequency
 - be aware of regulations surrounding maintenance, as indicated in BS5839-1, which dictate corrective maintenance actions
 - diagnostic techniques:
 - identify common faults and their potential causes in the system such as earth faults, open circuit faults and short circuit faults
 - reading and interpreting signals:
 - read and understand system displays and indicators to diagnose faults
 - use of technical documentation:
 - read and interpret system wiring diagrams and technical data
 - understand the importance of accurate record-keeping for maintenance activities and system performance history within a logbook

- When **maintaining intrusion alarms** technicians must understand:
 - the importance of testing detectors to ensure they operate as expected
 - the importance of testing outputs to ensure they operate as expected, such as bells, strobes and auxiliary devices
 - how to diagnose faults
 - responsibilities regarding false alarm management, including providing training to customers
 - different signalling paths and devices to ensure the system communicates as expected

- the importance of ensuring arming and disarming of the system
- the British Standard 9263:2016 - this is the standard for commissioning, maintenance and remote support of intruder and hold-up alarm systems
- the importance of inspection on the system to ensure compliance with regulations and manufacturer recommendations, including:
 - BS EN 50131
 - PD 6662
 - BS 8243
 - BS 7671

- When **maintaining access control systems** technicians must understand the importance of:
 - inspection on the system to ensure compliance with regulations and manufacturer recommendations, including:
 - BS EN 60839-11-2
 - Building Regulations: Part M
 - BS 7671
 - ensuring all doors are operating correctly and not impeded
 - testing all emergency egress and emergency release systems to function as expected
 - ensuring all requests to exit systems function as expected
 - having a basic understanding of BS EN 60839-11-2 regarding the maintenance of electronic access control systems

- When **maintaining video surveillance (CCTV)** technicians must understand the importance of:
 - ensuring all cameras are clear and have good image quality
 - checking all recording and playback functionality, ensuring the duration of recording is suitable
 - testing all additional supplement lighting, including white light and infra-red required for clear images in all environmental conditions
 - ensuring images are accessible to the Remote Video Response Centre (RVRC) or remote monitoring stations if applicable
 - having a basic understanding of BS EN 62676-4 regarding the maintenance of electronic access control systems
 - inspection of the system to ensure compliance with regulations and manufacturer recommendations, including:

- BS EN 62676-4
- BS 8418: installation and remote monitoring of detector activated CCTV systems - code of practice
- BS 7671

- **Principles and techniques for diagnostics and taking readings:**
 - diagnose common issues using system indicators and error messages
 - perform electrical testing to determine equipment failure, faulty wiring or terminations with a multimeter

- **Carrying out maintenance activities on intrusion alarm, access control, video surveillance (CCTV) involves completing:**
 - system inspection:
 - examine physical condition of cameras and housings
 - check for clear camera lens visibility
 - ensure accurate alignment and positioning of cameras
 - inspect cables and connections for damage
 - performance verification:
 - test image clarity and colour accuracy
 - confirm motion detection functionality
 - verify night vision and lighting levels
 - assess audio recording capabilities, if applicable
 - software and firmware:
 - update DVR/NVR firmware to the latest version
 - check for updates in camera firmware
 - review software settings for optimal performance
 - ensure cybersecurity measures are up to date
 - record keeping and compliance:
 - maintain logs of maintenance activities and system access

- review storage capacity and archive old footage
 - ensure compliance with data protection laws
 - document any system modifications or upgrades
- **Carrying out maintenance activities on fire detection and alarm systems** involves completing:
 - inspection and testing:
 - conduct visual checks for any physical damage or obstruction
 - test manual call points and detectors for functionality
 - test sounders and visual indications for functionality
 - test signalling to ensure signals are received by alarm receiving centre
 - system performance:
 - verify system compliance in relation to any changes to the building structure
 - ensure control panel displays are functioning and show correct system status
 - fault management:
 - log and address any system faults or irregularities
 - ensure backup power supplies are operational
 - documentation:
 - ensure records of all maintenance activities, faults and resolutions are documented
 - update system documentation to reflect any changes or upgrades

Environment and sustainability		
Knowledge	Skills	Behaviours
<p>K9 Environmental legislation: impact on fire and security systems processes and technologies.</p> <p>K14 Awareness of global carbon reduction needs and application of carbon reduction solutions.</p>	<p>S6 Comply with environmental and sustainability, regulations and standards.</p>	<p>B2 Takes personal responsibility for sustainable outcomes when carrying out duties, using industry and sector environmental best practices.</p>
Interview underpinned by a portfolio of evidence		
Pass criteria		Distinction criteria
<p>ES1 Explains how they comply with environmental and sustainability, regulations and standards to reduce the impact of fire and security systems processes and technologies on the environment (K9, S6)</p> <p>ES2 Explains how they take personal responsibility for sustainable outcomes in their work using industry and sector environmental best practices to support Global carbon reductions needs (K14, B2)</p>		<p><i>ES3 Explains how following their company procedures for sustainability reduces the impact of fire and security systems processes and technologies on the environment (K9, S6)</i></p>
Amplification and guidance		
<ul style="list-style-type: none"> • Environmental legislation and principles that technicians must comply with: <ul style="list-style-type: none"> ○ The Waste Electrical and Electronic Equipment Regulations ○ The Environment Act ○ The Controlled Waste (England and Wales) Regulations ○ Holding a Waste Carriers Licence ○ Following re-use and recycle procedures by disposing of equipment in suitable locations in an environmentally-friendly manner 		

- Having an awareness of asbestos, as this is a substance that technicians can easily be exposed to and contract significant health problems from
- **Application of carbon reduction solutions:**
 - electric vehicles:
 - use other sources of fuel for company cars and vans
 - electric, self-charging and hybrid vehicles can be used to reduce a company's carbon output
 - minimising journeys:
 - plan journeys in advance to reduce the vehicle's mileage and ultimately the carbon output
 - install GPS trackers to assist with journey planning and response times
 - working effectively:
 - understand what is required before proceeding to the job to ensure that the necessary equipment is to hand, to avoid repeated visits
- **Comply with environmental and sustainability, regulations:**
 - Waste Electrical Electronic Equipment (WEEE) Regulations – ensure that electronic items are disposed of correctly and in an environmentally-friendly manner. Distributors of electronic equipment often provide facilities for WEEE disposal.
 - Waste Carriers Licence – if carrying waste generated by yourself, it is important that you hold a Waste Carriers Licence. There are various tiers depending on how the waste is generated.
 - Control of Substances Hazardous to Health (COSHH) Regulations – comply with COSHH regulations to minimise the environmental harm caused and carry out risk assessments when using dangerous chemicals and substances.
 - Take responsibility and consider the correct use of resources and equipment to reduce the impact on environmental factors.
- **Takes personal responsibility for sustainable outcomes by:**
 - not being wasteful with equipment and materials
 - recycling and reusing where possible
 - following environmental best practices

- using sustainable products and materials
- being knowledgeable about ethical business practices
- being aware of waste segregation and regulations for hazardous substances, such as the Control of Substances Hazardous to Health (COSHH) Regulations

Customer service and stakeholder management

Knowledge	Skills	Behaviours
<p>K10 Principles of customer service: technicians' responsibilities, impact on brand, professional image and commercial risks.</p> <p>K16 Collaboration working techniques with internal and external stakeholders.</p>	<p>S10 Work collaboratively with internal and external stakeholders, as part of a team. Consult and engage with occupants or others who are or could be affected by work (for example vulnerable, older, and disabled people) and respond appropriately.</p>	<p>B6 Collaborates with others.</p>
Interview underpinned by a portfolio of evidence		
Pass criteria	Distinction criteria	
<p>CS1 Outlines their responsibilities for delivering customer service and the impact that this has on the organisations brand, professional image and commercial risks (K10)</p> <p>CS2 Explains how they work collaboratively with stakeholders as part of a team including consulting and engaging with occupants when undertaking work tasks (K16, S10, B6)</p>	<p>CS3 <i>Evaluates the benefits of working collaboratively with stakeholders, and the impact of not doing this on themselves, their stakeholders and the organisation (K16, S10)</i></p>	

Amplification and guidance

- **Principles of customer service** include:
 - building and maintaining relationships
 - managing conflict and dispute
 - offering sound and mutually productive information
 - providing advice and guidance
 - monitoring customer problems
 - avoiding the use of jargon
 - clearly explaining necessary information
 - following the General Data Protection Regulation (GDPR)
- **Professional image** can be maintained by:
 - remaining calm at all times and speaking to clients in a courteous manner
 - not getting angry or confrontational even when in a difficult situation
 - always keeping a tidy work environment
 - being punctual and reliable to achieve high-quality outcomes
- **Collaboration working techniques:**
 - communicate with stakeholders in a professional and diligent manner
 - keep relevant stakeholders informed of progress and any delays or issues
 - formulate action plans and work with stakeholders
- **Work collaboratively with internal and external stakeholders:**
 - consult with other members of the team and understand their needs and requirements
 - regularly update clients and other trades of progress
 - understand how to work in a safe manner to ensure the safety of yourself and others
- **Engage with occupants or others who are or could be affected by work:**
 - understand the Equality Act and how this may affect the installation of fire and security equipment, such as:

- the height of mountings
- the use of braille
- potential safeguarding issues
- the use of appropriate language to communicate
- recognise the specific needs of customers and cater to them
- **Collaborate with others** by:
 - working with other technicians, engineers and professionals within the team
 - creating open and clear communication with customers to understand their needs
 - working productively with colleagues and customers
 - positively engaging with suppliers and other external stakeholders
 - sharing best practices and knowledge with others team members
 - engaging in cross-functional projects

Communication	
Knowledge	Skills
<p>K11 Verbal communication techniques. Giving and receiving information. Adapting style to audience. Barriers in communication and how to overcome them. Sector specific terminology.</p> <p>K13 Written communication techniques: paper based and digital. Plain English principles. Sector specific terminology.</p>	<p>S9 Communicate with others verbally for example, internal and external customers, colleagues, and managers using sector specific terminology.</p> <p>S11 Communicate with internal and external stakeholders using sector specific terminology through written means.</p>

Interview underpinned by a portfolio of evidence	
Pass criteria	Distinction criteria
<p>CO1 Explains how they communicate verbally with internal and external stakeholders using techniques suitable for the context, adapting style and use of terminology to suit the audience (K11, S9)</p> <p>CO2 Explains how they communicate with internal and external stakeholders in written form using techniques suitable for the context and sector specific terminology (K13, S11)</p>	<p>CO3 Explains how they communicate verbally to agree an outcome when stakeholders have conflicting views (K11, S11)</p>
Amplification and guidance	
<ul style="list-style-type: none"> • Verbal communication techniques: <ul style="list-style-type: none"> ○ use clear and concise language to provide information effectively ○ avoid the use of jargon when speaking with customers ○ use active listening techniques to ensure accurate reception of information, such as repeating to confirm the information, and demonstrate listening with the use of verbal and nonverbal indicators • Adapting style to audience by: <ul style="list-style-type: none"> ○ using different communication styles depending on the audience ○ incorporating visual aids and examples to clarify complex concepts ○ tailoring communication to match the technical understanding of the recipient, including internal and external customers • Barriers in communication and how to overcome them: <ul style="list-style-type: none"> ○ identifying and addressing potential barriers such as disabilities, language differences and cultural backgrounds ○ use of communication strategies such as simplified language and use of visual and written aids to support understanding ○ use of technology to improve communication such as videos, translation software and digital content 	

- encouraging feedback to ensure the message is received as intended
- **Sector specific terminology:**
 - technicians should understand and utilise industry-specific jargon and acronyms to provide effective means of communication while also ensuring the audience's familiarity with the terms
 - specialised vocabulary should only be used for communication aimed at suitable audiences within the sector
 - technicians should provide explanations or alternatives when communicating with audiences that are not familiar with sector-specific terms or technical jargon to ensure inclusivity and understanding
 - examples of sector specific terminology include:
 - **PPE:** Personal Protective Equipment - safety wear for hazard protection
 - **IP Rating:** Ingress Protection - measures the enclosure's protection level
 - **DVR:** Digital Video Recorder - stores CCTV footage
 - **NVR:** Network Video Recorder - stores CCTV footage
 - **NSI:** National Security Inspectorate
 - **SSAIB:** Security Systems and Alarms Inspection Board
 - **BAFE:** British Approvals for Fire Excellence
 - **FIA:** Fire Industry Association - sector trade association
 - **PSU:** Power Supply Unit - provides power to security devices
 - **ATS:** Alarm Transmission Equipment
 - **End of Line:** a device - typically resistors or capacitors which are utilised to monitor a detection circuit
- **Written communication techniques:**
 - both traditional paper documents and modern digital platforms are used. This is dependent on the intended use, accessibility and its ability to meet the requirements of the organisation's intended audience. Examples of this include:
 - the use of paper documentation for fire logbooks, as entries can easily be added and it makes it difficult to edit existing entries
 - the use of digital documentation for commissioning paperwork, so that it is accessible to maintenance engineers for future visits

- written communication should aim for clarity, simplicity, and avoid jargon and complex sentences unless necessary.
- proofreading should be completed to eliminate spelling, grammar and punctuation errors.
- the information must be factual and up to date to maintain trust and confidence in what is provided.

- **Communicate with others verbally by:**
 - selecting the most effective communication method (face-to-face, phone call or video call) based on the intended message and the audience's preferences
 - using sector-specific terminology to convey complex ideas when addressing professionals within the sector
 - ensuring clarity by avoiding or explaining jargon to non-specialist audiences to prevent misunderstandings
 - using active listening techniques to understand the audience's perspective and respond appropriately
 - asking questions and giving feedback to ensure the message is understood and to address any areas of ambiguity
 - being mindful of cultural differences that may affect communication preferences and interpretations
 - considering the environment when choosing a communication method as it may not be suitable due to background noise level, confidentiality and distractions

- **Communicate with internal and external customers, colleagues, and managers by:**
 - identifying the audience to determine whether it consists of internal stakeholders (colleagues and managers) or external parties (customers and partners) and adjust communication accordingly.
 - assessing the audience's knowledge to gauge the level of familiarity with sector-specific terminology to tailor the communication effectively. Ensure not to automatically assume the audience's level of knowledge.
 - choose how formal or informal the communication should be based on the audience's position, relationship and the context of the communication.

- **Communicate with internal stakeholders through written means:**
 - internal stakeholder communication is typically more informal and uses sector-specific terms based on the recipient's role

- the method of communication is likely to differ based on the recipient, for example, clerical and office-based staff will use emails, while field-based staff will use mobile app platforms and messaging services
- written communication with internal stakeholders may not always been suitable - this is dependent upon the urgency of the message
- **Communicate with external stakeholders through written means:**
 - external stakeholder communication will typically be formal communication and less likely to use sector-specific terms, depending on the role of the recipient
 - ensure clarity by avoiding or explaining jargon to non-specialist audiences to prevent misunderstandings
 - the urgency and sensitivity of the information should be considered when choosing to communicate through written means

Equity, diversity and inclusion (EDI)	
Knowledge	Behaviours
K20 Equity, diversity and inclusion legislation and its impact in the fire and security safety sector.	B3 Promotes equity, diversity, and inclusivity in the workplace.
Interview underpinned by a portfolio of evidence	
Pass criteria	<i>Distinction criteria</i>
ED1 Explains how they follow equity, diversity and inclusion principles and legislative guidance and promote the principles to others (K20, B3)	ED2 <i>Explains the benefits of supporting a diverse and inclusive culture for the business</i> (K20)

Amplification and guidance

- **Equity, diversity and inclusion legislation:**
 - The Equality Act protects people from discrimination in the workplace. All parties within an organisation must follow this legislation.
- **Impact in the fire and security safety sector:**
 - systems must be designed and installed in ways that they do not disadvantage certain individuals, for example:
 - manual call points must be mounted at a height where wheelchair users can access them
 - equipment must be installed in a manner that does not disadvantage someone due to their disability or age
- **Promote equity, diversity, and inclusivity by:**
 - ensuring that systems are accessible to everyone
 - following the relevant legislations
 - using inclusive language
 - being sensitive and considerate to different cultures
 - understanding the different types of customers and their needs

Continuous professional development (CPD)

Behaviours

B4 Committed to **maintaining and enhancing competence** of self and others through **Continued Professional Development (CPD)**.

Interview underpinned by a portfolio of evidence	
Pass criteria	Distinction criteria
<p>CP1 Explains CPD they have undertaken and their future plans for CPD to enhance competence (B4)</p>	<p><i>No distinction criteria.</i></p>
Amplification and guidance	
<ul style="list-style-type: none"> • Continued Professional Development (CPD) is learning experiences that help an individual to develop and improve their professional practice. This is achieved through the acquirement and enhancement of skills, knowledge and experience. • Maintaining and enhancing competence can be achieved by: <ul style="list-style-type: none"> ○ completing online training ○ reading industry/trade magazines or online newsletters ○ completing in-house training sessions ○ attending manufacturer training courses ○ attending trade shows ○ staying informed on industry standards 	

[Click here to return to contents](#)

Assessment summary

The end-point assessment for the Fire, Emergency and Security Systems apprenticeship standard is made up of **3** assessment methods:

1. A multiple-choice test consisting of **60** multiple-choice questions of **75-minute** duration
2. A **9-hour (+10%)** practical assessment with questioning, of at least **3 questions**, consisting of **3** separate tasks
3. A **60-minute (+10%)** interview underpinned by a portfolio of evidence, of at least **6 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.

Multiple-choice test

All assessment methods are weighted equally. Total marks available are 60.

- To achieve a **pass**, apprentices will score at least 36 out of 60
- To achieve a **distinction**, apprentices must score at least 48 out of 60
- **Unsuccessful** apprentices will have scored 35 or below

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

Practical assessment with questioning

All assessment methods are weighted equally. The practical assessment with questioning is graded at pass only. Apprentices will be marked against the pass criteria outlined in this kit.

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

The practical assessment with questioning must take place in a simulated environment.

Interview underpinned by a portfolio of evidence

All assessment methods are weighted equally. 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 not have achieved all of the pass criteria

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

Grading

The apprenticeship includes pass and distinction grades, with the final grade based on the apprentice's combined performance in each assessment method.

To achieve a pass, the apprentice is required to pass each of the 3 assessment methods.

To achieve a distinction, the apprentice must achieve a distinction in the multiple-choice test and the interview underpinned by a portfolio of evidence and a pass in the practical assessment with questioning.

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

Practical assessment with questioning	Interview underpinned by a portfolio of evidence	Multiple-choice test	Overall grading
Fail	Any grade	Any grade	Fail
Any grade	Fail	Any grade	Fail
Any grade	Any grade	Fail	Fail
Pass	Pass	Pass	Pass
Pass	Distinction	Pass	Pass
Pass	Pass	Distinction	Pass
Pass	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.

A resit is typically taken within **3 months** of the EPA outcome notification. The timescale for a retake will be dependent on how much retraining is required but is typically taken within **6 months** of the EPA outcome notification.

When undertaking a resit or retake, the assessment method(s) will need to be reattempted in full, regardless of any individual assessment criteria that were passed on any prior attempt. However for the practical assessment with questioning, only the tasks failed will need to be resat or retaken. The EPA report will contain feedback on areas for development and resit or retake guidance.

Any EPA component resit/retake must be taken within a **6-month period**, otherwise the entire EPA must be retaken in full. Apprentices should have a supportive action plan to prepare for the resit/retake.

Apprentices who achieve a pass grade cannot resit or retake the EPA to achieve a higher grade.

Where any assessment method has to be resat or retaken, the apprentice will be awarded a maximum grade of pass, 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 multiple-choice test

The test consists of **60 multiple-choice questions** and will last **75 minutes**. The **pass** mark is 36 out of 60 and the **distinction** mark is 48 out of 60.

The apprentice will have **at least 2 weeks'** notice of the date and time of the test.

The multiple-choice 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.

Multiple-choice test criteria

Multiple-choice test

K1 Awareness of Health and safety legislations, codes of practice and safe working practices, relevant to the occupation and the operative's responsibilities. Including Health and Safety at Work Act, BS 7671, BS EN 50131, BS EN 62676 and BS 5839.

K2 Testing techniques for electrical and electronic components used in fire detection and alarm systems. The principles of using meters, applying Ohms law, formulae, calculations and taking readings.

K3 The principles of fire detection and fire alarm systems: features and design criteria, survey methods and impact on the fire safety industry.

K7 Principles of planning and project management of fire and security system installation: commissioning, and handover.

K8 Data collection, storage and sharing methods and techniques.

K12 Principles and techniques for installing and maintaining electronic systems: SI units, quantities, formulae and calculations, electromagnetism and electromagnetic induction, ICT applications, smart Apps and power supplies.

K15 Testing techniques for electrical and electronic components used in intrusion alarms, access control systems and video surveillance systems (CCTV). The principles of using meters, applying Ohms Law, formulae, calculations and taking readings.

K17 Techniques for planning and installing systems cabling; methods of containment and protection.

K19 The principles of intrusion alarms, access control, video surveillance (CCTV) features and design criteria, survey methods and impact on the building security industry.

[Click here to return to contents](#)

Assessing the practical assessment with questioning

In the practical assessment with questioning, an assessor will observe the apprentice completing a series of tasks. This will take place in a stimulated environment that closely relates to the apprentice's natural working environment.

The apprentice will have **2 weeks'** notice of the practical assessment with questioning.

The practical assessment with questioning must take **9 hours**. The assessor can increase the time by up to **10%** to allow the apprentice to complete a task or respond to a question if necessary. It may take place in parts, but it must be completed over 2 consecutive working days. A working day is considered to be 7.5 hours long.

The assessor will brief the apprentice on the format and timescales of the practical assessment with questioning before it starts. The time taken for this briefing is not included in the assessment time.

Questioning can occur both during and after the practical assessment. The time for questioning is included in the overall assessment time. To remain as unobtrusive as possible, the assessor will ask questions during natural stops between tasks and after completion of work rather than disrupting the apprentice's flow.

The assessor will ask a **minimum of 3 questions**. Follow-up questions will be asked where required and are in addition to the set number of questions.

The practical test with questioning must be relevant to the apprentice's day-to-day duties. There are 2 options: fire systems tasks and security systems tasks.

Where the apprentice's daily duties relate to fire systems, the independent assessor must observe **3** separate tasks based on prepared addressable and non-addressable fire alarm systems during the practical assessment.

Where the apprentice's daily duties relate to security systems, the independent assessor must observe **3** separate tasks based on an access control system, intrusion alarm system and video surveillance system during the practical assessment.

The tasks for both of these options are below.

Fire systems task 1: Takeover a system (2.5 hours)

This task requires the apprentice to interpret and follow a written brief for the takeover, fault identification and rectification activity to be carried out on an addressable and non-addressable fire system.

The system must contain, as a minimum:

- a prepared addressable fire alarm system
- a prepared non-addressable fire alarm system

- 5 preset faults installed by the independent assessor in the prepared addressable fire alarm system, including a non-compliance to British Standards
- 5 preset faults installed by the independent assessor in the prepared non-addressable fire alarm system, including a non-compliance to British Standards

The apprentice will be observed carrying out takeover procedures including:

- complying with health and safety
- carrying out risk assessments
- carrying out takeover procedures for prepared addressable and non-addressable fire alarm systems
- carrying out fault diagnosis activities for prepared addressable and non-addressable fire alarm systems
- recording findings, making recommendations and rectifying the faults and non-compliances identified in the prepared addressable and non-addressable fire alarm systems

Fire systems task 2: Additions to systems (4.5 hours)

This task requires the apprentice to make additions to prepared addressable and non-addressable fire alarm system installations.

The system must contain, as a minimum a:

- prepared addressable fire alarm system to which a minimum of 3 components and systems cabling can be added
- prepared non-addressable fire alarm system to which a minimum of 3 components and systems cabling can be added

The apprentice will be observed carrying out additions to systems procedures including:

- complying with health and safety regulations
- carrying out additions to the system's procedures and configurations, including systems cabling for a prepared addressable alarm system
- carrying out additions to the system's procedures and configurations, including systems cabling for a non-addressable fire alarm system

Fire systems task 3: Commission systems (2 hours)

This task requires the apprentice to commission, test and handover the prepared addressable and non-addressable fire alarm systems.

The system must contain, as a minimum a:

- prepared addressable fire alarm system including additions made during task 2 of the practical test
- prepared non-addressable fire alarm system including additions made during task 2 of the practical test

The apprentice will be observed carrying out commissioning, testing and handover procedures including:

- complying with health and safety regulations
- completing commissioning and testing activities of a prepared addressable fire alarm system, including additions made during component 2 of the practical test
- completing commissioning and testing activities of a prepared non-addressable fire alarm system, including additions made during component 2 of the practical test
- completing the handover procedure for a prepared addressable fire alarm system
- completing the handover procedure for a prepared non-addressable fire alarm system

Security systems task 1: Takeover a system (2.5 hours)

This task requires the apprentice to interpret and follow a written brief detailing the takeover, fault identification and rectification activity to be carried out on an access control system, intrusion alarm system and video surveillance system.

The system must contain, as a minimum:

- a prepared access control system
- a prepared intrusion alarm system
- a prepared video surveillance system
- 3 preset faults installed by the independent assessor in the prepared access control system, including 1 non-compliance to British Standards
- 3 preset faults installed by the independent assessor in the prepared intrusion alarm system, including 1 non-compliance to British Standards
- 3 preset faults installed by the independent assessor in the prepared video surveillance system, including 1 non-compliance to British Standards

The apprentice will be observed carrying out takeover procedures including:

- complying with health and safety regulations
- carrying out risk assessments
- carrying out procedures for prepared access control, intrusion alarm and video surveillance systems

- carrying out fault diagnosis activities for prepared access control, intrusion alarm and video surveillance systems
- recording findings, making recommendations and rectifying faults and non-compliances identified in the prepared access control, intrusion alarm and video surveillance systems

Security systems task 2: Additions to systems (4.5 hours)

This task will require the candidate to make additions to an access control system, intrusion alarm system and video surveillance system installations.

The system must contain, as a minimum a:

- prepared access control system
- prepared intrusion alarm system
- prepared video surveillance system

The apprentice will be observed carrying out additions procedures including:

- complying with health and safety regulations
- carrying out additions to the access control system: a minimum of 2 additions including systems cabling
- carrying out additions to an intrusion alarm system: a minimum of 2 additions including systems cabling
- carrying out additions to a video surveillance system: a minimum of 2 additions including systems cabling

Security systems task 3: Commission systems (2 hours)

This component requires the apprentice to commission, test and handover the prepared access control, intrusion alarm and video surveillance systems.

The system must contain, as a minimum a:

- prepared access control system, including additions made during task 2 of the practical test
- prepared intrusion alarm system, including additions made during task 2 of the practical test
- prepared video surveillance system, including additions made during task 2 of the practical test

The apprentice will be observed carrying out and documenting commissioning, specified tests and handover procedures including:

- complying with health and safety regulations

- completing commissioning and specified tests of a prepared access control system, including additions made during task 2 of the practical test
- completing commissioning and specified tests of a prepared access intrusion alarm system, including additions made during task 2 of the practical test
- completing commissioning and specified tests of a prepared video surveillance system, including additions made during task 2 of the practical test
- completing the handover procedures for a prepared access control system
- completing the handover procedures for a prepared intrusion alarm system
- completing the handover procedures for a prepared video surveillance system

Before the assessment

Employers/training providers should:

- ensure the apprentice knows the date, time and location of the assessment
- ensure the apprentice knows which fire, emergency and security system technician 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

Grading the practical assessment with questioning

The practical assessment with questioning is graded at a pass only. Apprentices will be marked against the pass criteria included in the tables on the following pages (under 'Practical assessment with questioning criteria').

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

Practical assessment with questioning 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 practical assessment with questioning 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 practical assessment with questioning should take place in a suitable location.
- a 9-hour time slot should be available for the practical assessment with questioning, if it is intended to be a complete mock practical assessment with questioning 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 practical assessment with questioning 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 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:
 - outline how you prioritise workplace health and safety when working
 - tell me how you use digital information systems and which principles you follow while doing this
 - describe how you ensure that you are working in line with the task's requirements

Practical assessment with questioning criteria

Throughout the **9-hour** practical assessment with questioning, the assessor will review the apprentice's competence in the criteria outlined below.

Apprentices should prepare for the practical assessment with questioning by considering how the criteria can be met.

Health and safety

To pass, the following must be evidenced in task 1, 2 and 3.

HS1 Prioritises workplace health, safety and wellbeing and complies with health and safety regulations, standards and guidance in line with the task requirements (S1, B1)

Diagnostics and fault finding

To pass, the following must be evidenced in task 1.

DF1 Carries out takeover procedures and applies diagnostics techniques prior to repairing faults in line with the task requirements and manufacturer's instructions (S4)

Risk assessments

To pass, the following must be evidenced in task 1, 2 and 3.

RA1 Carries out risk assessments in line with the task requirements, organisational procedures and legal and regulatory requirements (K5, S8)

Commissioning, testing and handover

To pass, the following must be evidenced in task 3.

CT1 Completes functionality tests of systems and components during commissioning and handover in line with the task requirements and manufacturer's instructions (S2, S7)

CT2 Uses digital information systems to store, retrieve, manipulate, transmit and receive digital data and electronic information in line with the task requirements following legal and regulatory guidance, GDPR and ethical principles (K18, S5, B5)

Installation

To pass, the following must be evidenced in task 2.

IN1 Plans and installs systems cabling, in line with the task requirements, manufacturer's instructions and legal and regulatory requirements (S12)

IN2 Applies and implements system design, in line with the task requirements, manufacturer's instructions and legal and regulatory requirements (S3)

[Click here to return to contents](#)

Assessing the interview underpinned by a portfolio of evidence

In the interview underpinned by a portfolio of evidence, the assessor asks the apprentice questions to assess their competence against the relevant criteria outlined in this kit.

Apprentices will have access to their portfolio during the interview. They can refer to and illustrate their answers with evidence from their portfolio of evidence during the interview. However, the portfolio of evidence is not directly assessed.

The apprentice will have **2 weeks'** notice of the interview underpinned by a portfolio of evidence.

It will take place in a suitable environment and can be conducted by video conferencing. It will last for **60 minutes**. The independent assessor can increase the time of the interview underpinned by a portfolio of evidence by up to **10%** to allow the apprentice to respond to a question if necessary.

The assessor will ask **at least 6 questions**. Follow-up questions will be asked where clarification is required. The purpose of the questions is to assess the following themes:

- fire, alarm and security system maintenance
- environment and sustainability
- customer service and stakeholder management
- equity, diversity and inclusion (EDI)
- continuous professional development (CPD)
- communication

Before the assessment

Employers/training providers should:

- ensure the apprentice knows the date, time and location of the assessment
- ensure the apprentice knows which criteria will be assessed (outlined on the following pages)
- ensure that the apprentice has access to their portfolio of evidence during the interview
- encourage the apprentice to reflect on their experience and learning on-programme to understand what is required to meet the standard
- be prepared to provide clarification to the apprentice, and signpost them to relevant parts of their on-programme experience as preparation for this assessment

Grading the interview underpinned by a portfolio of evidence

Apprentices will be marked against the pass and distinction criteria included in the tables on the following pages (under 'Interview underpinned by a portfolio of evidence criteria').

- 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

Interview underpinned by a portfolio of evidence 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 interview underpinned by a portfolio of evidence in preparation for the real thing. The most appropriate form of mock interview underpinned by a portfolio of evidence 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 interview underpinned by a portfolio of evidence should take place in a suitable location.
- a 60-minute time slot should be available to complete the interview underpinned by a portfolio of evidence, if it is intended to be a complete interview 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 interview underpinned by a portfolio of evidence 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 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:
 - system maintenance

- Describe how maintenance is carried out on fire detection and alarm systems
- environment and sustainability
 - Explain how you work to promote sustainability
- customer service and stakeholder management
 - Outline the impact that poor customer service can have on an organisation
- communication
 - Explain a time that you have adapted your communication style when talking to an external stakeholder
- equity, diversity and inclusion (EDI)
 - Outline some benefits of supporting diversity and inclusion principles
- continuous professional development (CPD)
 - Describe the continuous professional development (CPD) that you have undertaken

Interview underpinned by a portfolio of evidence criteria

Throughout the **60-minute** interview underpinned by a portfolio of evidence, the assessor will review the apprentice's competence in the criteria outlined below.

Apprentices should prepare for the interview underpinned by a portfolio of evidence by considering how the criteria can be met.

System maintenance
To pass, the following must be evidenced.
SM1 Describes how they carry out maintenance activities on fire detection and alarm systems and their components in line with manufacturer's guidance, organisational procedures and legislative regulations and guidance (K4, S13)
SM2 Describes how they carry out maintenance activities on intrusion alarm, access control, video surveillance (CCTV) and their components in line with manufacturer's guidance, organisational procedures and legislative regulations and guidance (K6, S14)
To gain a distinction, the following must be evidenced.
SM3 Explains the importance to the customer and the organisation of following manufacturer's guidance, organisational procedures and legislative regulations and guidance when maintaining fire detection and fire safety systems and components (K4, S13)
SM4 Explains the importance to the customer and organisation of following manufacturer's guidance, organisational procedures and legislative regulations and guidance when maintaining intrusion alarm, access control, video surveillance (CCTV) and their components (K6, S14)

Environment and sustainability
To pass, the following must be evidenced.
ES1 Explains how they comply with environmental and sustainability, regulations and standards to reduce the impact of fire and security systems processes and technologies on the environment (K9, S6)
ES2 Explains how they take personal responsibility for sustainable outcomes in their work using industry and sector environmental best practices to support Global carbon reductions needs (K14, B2)
To gain a distinction, the following must be evidenced.
ES3 Explains how following their company procedures for sustainability reduces the impact of fire and security systems processes and technologies on the environment (K9, S6)

Customer service and stakeholder management

To pass, the following must be evidenced.

CS1 Outlines their responsibilities for delivering customer service and the impact that this has on the organisations brand, professional image and commercial risks (K10)

CS2 Explains how they work collaboratively with stakeholders as part of a team including consulting and engaging with occupants when undertaking work tasks (K16, S10, B6)

To gain a distinction, the following must be evidenced.

CS3 Evaluates the benefits of working collaboratively with stakeholders, and the impact of not doing this on themselves, their stakeholders and the organisation (K16, S10)

Communication

To pass, the following must be evidenced.

CO1 Explains how they communicate verbally with internal and external stakeholders using techniques suitable for the context, adapting style and use of terminology to suit the audience (K11, S9)

CO2 Explains how they communicate with internal and external stakeholders in written form using techniques suitable for the context and sector specific terminology (K13, S11)

To gain a distinction, the following must be evidenced.

CO3 Explains how they communicate verbally to agree an outcome when stakeholders have conflicting views (K11, S11)

Equity, diversity and inclusion (EDI)

To pass, the following must be evidenced.

ED1 Explains how they follow equity, diversity and inclusion principles and legislative guidance and promote the principles to others (K20, B3)

To gain a distinction, the following must be evidenced.

ED2 Explains the benefits of supporting a diverse and inclusive culture for the business (K20)

Continuous professional development (CPD)

To pass, the following must be evidenced.

CP1 Explains CPD they have undertaken and their future plans for CPD to enhance competence (B4)

To gain a distinction, the following must be evidenced.

No distinction criteria.

[Click here to return to contents](#)