ST1401/V

DRAFT END-POINT ASSESSMENT PLAN FOR ST1401 PROTECTIVE SECURITY ADVISER APPRENTICESHIP

Introduction and overview

This document explains the requirements for end-point assessment (EPA) for the protective security adviser apprenticeship. End-point assessment organisations (EPAOs) must follow this when designing and delivering the EPA.
Protective Security Adviser apprentices, their employers and training providers should read this document.
A full-time protective security adviser apprentice typically spends 18 months on-programme. The apprentice must spend at least 12 months on-programme and complete the required amount of off-the-job training in line with the apprenticeship funding rules.
The EPA should be completed within an EPA period lasting typically 5 months.
The apprentice must complete their training and meet the gateway requirements before starting their EPA. The EPA will assess occupational competence.

An approved EPAO must conduct the EPA for this apprenticeship. Employers must work with the training provider to select an approved EPAO from the apprenticeship providers and assessment register (APAR).
This EPA has 2 assessment methods.
The grades available for each assessment method are below.

Assessment method 1 - project report with presentation:

- fail
- pass
- distinction

Assessment method 2 - professional discussion underpinned by a portfolio of evidence:

- fail
- pass
- distinction

The result from each assessment method is combined to decide the overall apprenticeship grade. The following grades are available for the apprenticeship:

- fail
- pass
- merit
- distinction

EPA summary table

On-programme - typically 18 months	The apprentice must: • complete training to develop the knowledge, skills and behaviours (KSBs) outlined in this apprenticeship's standard • complete training towards English and mathematics qualifications in line with the apprenticeship funding rules • compile a portfolio of evidence
End-point assessment gateway	The apprentice's employer must be content that the apprentice is occupationally competent. The apprentice must: • confirm they are ready to take the EPA • have achieved English and mathematics qualifications in line with the apprenticeship funding rules For the professional discussion underpinned by a portfolio of evidence, the apprentice must submit a portfolio of evidence. Gateway evidence must be submitted to the EPAO, along with any organisation specific policies and procedures requested by the EPAO.
End-point assessment - typically 5 months	**The grades available for each assessment method are below** Project report with presentation: • fail • pass • distinction Professional discussion underpinned by a portfolio of evidence: • fail • pass • distinction **Overall EPA and apprenticeship can be graded:** • fail • pass • merit • distinction
Re-sits and re-takes	The details for re-sits and re-takes are below: • re-take and re-sit grade cap: pass • re-sit timeframe: typically 2 months • re-take timeframe: typically 3 months

Duration of end-point assessment period

The EPA is taken in the EPA period. The EPA period starts when the EPAO confirms the gateway requirements have been met and is typically 5 months.
The EPAO should confirm the gateway requirements have been met and start the EPA as quickly as possible.

EPA gateway

The apprentice's employer must be content that the apprentice is occupationally competent. That is, they are deemed to be working at or above the level set out in the apprenticeship standard and ready to undertake the EPA. The employer may take advice from the apprentice's training provider, but the employer must make the decision. The apprentice will then enter the gateway.
The apprentice must meet the gateway requirements before starting their EPA.

They must:

- confirm they are ready to take the EPA
- have achieved English and mathematics qualifications in line with the apprenticeship funding rules
- submit a portfolio of evidence for the professional discussion underpinned by a portfolio of evidence

Portfolio of evidence requirements:
The apprentice must compile a portfolio of evidence during the on-programme period of the apprenticeship. It should only contain evidence related to the KSBs that will be assessed by the professional discussion. It will typically contain 15 discrete pieces of evidence. Evidence must be mapped against the KSBs. Evidence may be used to demonstrate more than one KSB; a qualitative as opposed to quantitative approach is suggested.
Evidence sources may include workplace documentation and records, for example:

- workplace documentation and records
- workplace policies and procedures
- witness statements
- non sensitive annotated photographs

Any submitted work output must be **redacted to remove any commercially sensitive or personal information.**
This is not a definitive list; other evidence sources can be included.
The portfolio of evidence 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 evidence provided should be valid and attributable to the apprentice; the portfolio of evidence should contain a statement from the employer and apprentice confirming this.
The EPAO should not assess the portfolio of evidence directly as it underpins the discussion. The independent assessor should review the portfolio of evidence to prepare questions for the discussion. They are not required to provide feedback after this review.

Gateway evidence must be submitted to the EPAO, along with any organisation specific policies and procedures requested by the EPAO.

Order of assessment methods

The assessment methods must be delivered in the following order:

- Project with Presentation followed by Professional Discussion
- The rationale for this order of assessments is based in the natural order of the apprentice's workflow.

Project report with presentation

Overview

The project assessment method involves the apprentice completing a significant and defined piece of work that has a real business application and benefit. This process may include for example, research, analysis and the completion of tasks or activities to achieve the outcome. The assessment method will have an output at the end of the defined piece of work. The work completed for the project assessment method must meet the needs of the employer's business and be relevant to the apprentice's occupation and apprenticeship.

This assessment method has 2 components:

- completion of the defined piece of work for the project with a project output
- completion of the defined piece of work for the presentation with questions and answers

Together, these components give the apprentice the opportunity to demonstrate the KSBs mapped to this assessment method. They are assessed by an independent assessor.

Rationale

This assessment method is being used because:

- it allows for the assessment of KSBs that take place over a long period of time
- it allows for a broad set of KSBs to be evidenced during the post-gateway period
- it assesses KSBs holistically
- it can produce something that is of genuine business benefit to the apprentice's employer
- it allows the apprentice to directly demonstrate KSBs relating to communication and presentation
- it allows for the presentation of evidence and testing of responses where there are a range of potential answer
- it can be conducted remotely, potentially reducing cost

Delivery

The apprentice must complete a project based on the following:

- Converged protective security risk assessment
- it will cover the following themes:
    - cyber security
    - people security
    - personnel security
    - physical security
    - risk management
    - technical security
    - threat management

The EPAO must provide a project assessment method specification. It must detail how a project can enable an apprentice to meet the KSBs mapped to this assessment method to the highest available grade. The EPAO must also provide suggested project titles.
The project output must be in the form of a report and presentation.

The apprentice must start the project after the gateway. The employer should ensure the apprentice has the time and resources, within the project period, to plan and complete their project.

The apprentice may work as part of a team to complete the project, which could include internal colleagues or technical experts. The apprentice must however, complete their project report and presentation unaided and they must be reflective of their own role and contribution. The apprentice and their employer must confirm this when the report and any presentation materials are submitted.

Component 1: Project report

The project report must be based on a completed converged risk assessment, which must be submitted alongside the project report. The converged risk assessment must be **redacted to remove any commercially sensitive or personal information.**
The report must include at least:

- an executive summary (or abstract)
- an introduction
- the scope of the project (including key performance indicators, aims and objectives)
- a project plan
- research outcomes
- data analysis outcomes
- project outcomes
- discussion of findings
- recommendations and conclusions
- references
- appendix containing mapping of KSBs to the report.

The project report must have a word count of 4000 words. A tolerance of 10% above or below is allowed at the apprentice's discretion. Appendices, references and diagrams are not included in this total. The apprentice must produce and include a mapping in an appendix, showing how the report evidences the KSBs mapped to this assessment method. The apprentice must complete and submit the report and any presentation materials to the EPAO by the end of week 12 of the EPA period.

Component 2: Presentation with questions

The presentation with questions must be structured to give the apprentice the opportunity to demonstrate the KSBs mapped to this assessment method to the highest available grade.

The apprentice must prepare and deliver a presentation to an independent assessor. After the presentation, the independent assessor must ask the apprentice questions about their project, report and presentation.

The presentation will cover the following themes

- communication

The presentation should cover:

- an overview of the project
- the project scope (including key performance indicators)
- summary of actions undertaken by the apprentice
- project outcomes and how these were achieved

The presentation with questions must last 60 minutes. This will typically include a presentation of 15 minutes and questioning lasting 45 minutes. The independent assessor must use the full time available for questioning. The independent assessor can increase the time of the presentation and questioning by up to 10%. This time is to allow the apprentice to complete their last point or respond to a question if necessary.
The independent assessor must ask at least 8 questions. They must use the questions from the EPAO's question bank or create their own questions in line with the EPAO's training. Follow up questions are allowed where clarification is required.
The purpose of the independent assessor's questions is:

- to verify that the activity was completed by the apprentice
- to seek clarification where required
- to assess those KSBs that the apprentice did not have the opportunity to demonstrate with the report, although these should be kept to a minimum
- to assess level of competence against the grading descriptors

The apprentice must submit any presentation materials to the EPAO at the same time as the report - by the end of week 12 of the EPA period. The apprentice must notify the EPAO, at that point, of any technical requirements for the presentation.
During the presentation, the apprentice must have access to:

- audio-visual presentation equipment
- flip chart and writing and drawing materials

- computer

The independent assessor must have at least 2 weeks to review the project report and any presentation materials, to allow them to prepare questions.
The apprentice must be given at least 2 weeks' notice of the presentation with questions. The apprentice may choose to end the presentation early. The apprentice must be confident they have demonstrated competence against the assessment requirements for the assessment method. The independent assessor or EPAO must ensure the apprentice is fully aware of all assessment requirements. The independent assessor or EPAO cannot suggest or choose to end the assessment methods early, unless in an emergency. The EPAO is responsible for ensuring the apprentice understands the implications of ending an assessment early if they choose to do so. The independent assessor may suggest the assessment continues. The independent assessor must document the apprentice's request to end the assessment early.

Assessment decision

The independent assessor must make the grading decision. They must assess the project components holistically when deciding the grade.

The independent assessor must keep accurate records of the assessment. They must record:

- the KSBs demonstrated in the report and presentation with questions
- the apprentice's answers to questions
- the grade achieved

Assessment location

The presentation with questions must take place in a suitable venue selected by the EPAO for example, the EPAO's or employer's premises. It should take place in a quiet room, free from distractions and influence.

The presentation with questions can be conducted by video conferencing. The EPAO must have processes in place to verify the identity of the apprentice and ensure the apprentice is not being aided.

Question and resource development

The EPAO must develop a purpose-built assessment specification and question bank. It is recommended this is done in consultation with employers of this occupation. The EPAO must maintain the security and confidentiality of EPA materials when consulting with employers. The assessment specification and question bank must be reviewed at least once a year to ensure they remain fit-for-purpose.

The assessment specification must be relevant to the occupation and demonstrate how to assess the KSBs mapped to this assessment method. The EPAO must ensure that questions are refined and developed to a high standard. The questions must be unpredictable. A question bank of sufficient size will support this.

The EPAO must ensure that the apprentice has a different set of questions in the case of re-sits or re-takes.

EPAO must produce the following materials to support the project:

- independent assessor EPA materials which include:
  - training materials
  - administration materials
  - moderation and standardisation materials
  - guidance materials
  - grading guidance
  - question bank
- EPA guidance for the apprentice and the employer

The EPAO must ensure that the EPA materials are subject to quality assurance procedures including standardisation and moderation.

Professional discussion underpinned by a portfolio of evidence

Overview

In the professional discussion, an independent assessor and apprentice have a formal two-way conversation. It gives the apprentice the opportunity to demonstrate the KSBs mapped to this assessment method.

Rationale

This assessment method is being used because:

- it assesses KSBs holistically and objectively
- it allows for the assessment of KSBs that do not occur on a predictable or regular basis
- it allows for assessment of responses where there are a range of potential answers
- it can be conducted remotely, potentially reducing cost

Delivery

The professional discussion must be structured to give the apprentice the opportunity to demonstrate the KSBs mapped to this assessment method to the highest available grade.
An independent assessor must conduct and assess the professional discussion.
The purpose of the independent assessor's questions will be to assess the apprentice's competence against the following themes:

It will include the following themes:

- analysis
- communication
- legislation
- governance

- response management
- standards
- personal security

The EPAO must give an apprentice 2 weeks' notice of the professional discussion.
The independent assessor must have at least 2 weeks to review the supporting documentation.
The apprentice must have access to their portfolio of evidence during the professional discussion.
The apprentice can refer to and illustrate their answers with evidence from their portfolio of evidence however, the portfolio of evidence is not directly assessed.
The professional discussion must last for 60 minutes. The independent assessor can increase the time of the professional discussion by up to 10%. This time is to allow the apprentice to respond to a question if necessary.
The independent assessor must ask at least 10 questions. The independent assessor must use the questions from the EPAO's question bank or create their own questions in line with the EPAO's training. Follow-up questions are allowed where clarification is required.
The apprentice may choose to end the assessment method early. The apprentice must be confident they have demonstrated competence against the assessment requirements for the assessment method. The independent assessor or EPAO must ensure the apprentice is fully aware of all assessment requirements. The independent assessor or EPAO cannot suggest or choose to end the assessment methods early, unless in an emergency. The EPAO is responsible for ensuring the apprentice understands the implications of ending an assessment early if they choose to do so. The independent assessor may suggest the assessment continues. The independent assessor must document the apprentice's request to end the assessment early.
The independent assessor must make the grading decision.
The independent assessor must keep accurate records of the assessment. They must record:

- the apprentice's answers to questions
- the KSBs demonstrated in answers to questions
- the grade achieved

Assessment location

The professional discussion must take place in a suitable venue selected by the EPAO for example, the EPAO's or employer's premises.
The professional discussion can be conducted by video conferencing. The EPAO must have processes in place to verify the identity of the apprentice and ensure the apprentice is not being aided.
The professional discussion should take place in a quiet room, free from distractions and influence.

Question and resource development

The EPAO must develop a purpose-built assessment specification and question bank. It is recommended this is done in consultation with employers of this occupation. The EPAO must maintain the security and confidentiality of EPA materials when consulting with employers. The assessment specification and question bank must be reviewed at least once a year to ensure they remain fit-for-purpose.
The assessment specification must be relevant to the occupation and demonstrate how to assess the KSBs mapped to this assessment method. The EPAO must ensure that questions

are refined and developed to a high standard. The questions must be unpredictable. A question bank of sufficient size will support this.
The EPAO must ensure that the apprentice has a different set of questions in the case of re-sits or re-takes.
The EPAO must produce the following materials to support the professional discussion underpinned by a portfolio of evidence:

- independent assessor assessment materials which include:
  - training materials
  - administration materials
  - moderation and standardisation materials
  - guidance materials
  - grading guidance
  - question bank
- EPA guidance for the apprentice and the employer

The EPAO must ensure that the EPA materials are subject to quality assurance procedures including standardisation and moderation.

Grading

Project report with presentation

Fail - does not meet pass criteria

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
Communication K54 K57 K59 S29 S32 S34	Creates and delivers a presentation, applying communication strategies, language and style that maximises understanding and supports the achievement of goals and objectives. (K54, K57, K59, S29, S32, S34)	Innovatively combines communication strategies, presentation skills and influencing techniques to maximise understanding and achieve the intended purpose. (K57, K59, S32, S34)
Cyber Security K37 K38 K39 K40 K41 K42 K43 K44 K45 K46 S20 S21 S22	Reviews assessments of cyber threat vectors that could be used by threat actors to exploit vulnerabilities in organisational assets to create disruption to processes and creates mitigations to protect the confidentiality, integrity	Justifies how proposed mitigations protects confidentiality, integrity and availability of data and prevents cyber threat vectors. (K37, S20) Justifies how proposed mitigations prevent data

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
	and availability of data (K37, K38, K39, S20) Applies principles of encryption, cryptography, asymmetric cryptography, encryption keys, secure web browsing, and methods to protect data on the network when creating mitigations to prevent data loss with consideration of potential vulnerabilities and common network security threats and insider threats on data loss. (K42, K43, K44, S21) Illustrates how good password practice and salting in collaboration with hashing, alongside use of hardware tokens assist in the mitigation of hashing and brute force attack. (K45, K46, S22)	loss within the organisation. (K42, S21)
People Security K28 S16 B1	Develops mitigations against hostile reconnaissance to project a strong security posture by applying the principles of hostile reconnaissance, hostile planning stages, NPSA DENY, DETECT and DETER strategy, the integration of Security Minded Communications, See Check and Notify (SCaN) and Project Servator. (K28, S16, B1)	Evaluates how the principles of hostile reconnaissance were applied in the development of mitigations to protect the organisation against hostile reconnaissance. (K28, S16)
Personnel Security K25 K26 K27 S15	Develops mitigations against insider risks through	Analyses how different event typologies and

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
	organisational risk assessments, consideration of methods used by insiders and insider event typologies, the current threat landscape and societal challenges that influence the motivations of insiders, and the integration of personnel, cyber and physical controls. (K25, K26, K27, S15)	combinations of personnel, cyber, physical and technical security control measures best mitigate insider risk for organisations. (K26, K27, S15)
Physical Security K17 K18 K19 K20 K21 K22 K23 K24 S12 S13 S14	Creates physical security mitigations against marauding terrorist attacks using a combination of (LPS) 1673, LPS 1178 Issue 8, NPSA Marauding Terrorist Attack Standard, NPSA Manual Forced Entry Standards and ISO 22343-1:2023 Hostile Vehicle Mitigation to include attacks on glazing systems; attacks using a Vehicle as a Weapon (VAW); Vehicle Borne Improvised Explosive Device (VBIED) and the Layered Vehicle Attack using recommended methodologies to save lives. (K17, K18, K19, K20, K21, S12) Assesses surreptitious attack vectors using the principles of the NPSA Surreptitious Threat Mitigation Process and develop mitigations against surreptitious attack vectors. (K22, S13) Creates mitigations for security risks selecting and justifying the chosen	Substantiates how recommended forcible attack vector mitigations were developed in line with common security standards. (K19, K20, S12) Compares and contrasts physical security products and standards and their appropriateness for developing mitigations for different protective security risks. (K24, S14)

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
	combinations of governmental, independent and third party certified physical security products and drawing on the principles of the cyber assurance of physical security systems. (K23, K24, S14)	
Risk Management K1 K2 K3 K4 K10 K14 K15 K16 K51 K52 S1 S2 S8 S10 S11 S27	Applies crime and security theories and NTAs guidance to organisational protective security design to address protective security requirements and meet organisational needs. (K1, K2, S1) Applies the principles of security convergence to mitigate the vulnerabilities of a siloed approach to protective security design. (K3, K4, S2) Applies principles of asset identification and classification to produce organisational asset registers. (K10, S8) Applies the principles of security risk management and explains how these are applied when assessing the vulnerability of an organisation including how threat, vulnerability and impact determines the risk posed to an organisation, its assets and people and how mitigating the threat, vulnerabilities and impact can	Compares and contrasts the different roles NTAs play when addressing organisational protective security requirements. (K2, S1) Evaluates the strengths and weaknesses of quantitative, qualitative and semi-qualitative risk assessment. (K15, S11)

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
	be supported with protective security. (K14, S10) Develops risk statements and risk registers that support operational requirements, that includes Threat Actors, Assets Targeted, Attack Vectors used, and potential impact aligned to organisational assets, threat, vulnerability and impact, using quantitative, qualitative and semi-qualitative risk assessment methodologies. (K15, K16, S11) Explains how sustainable working practises have been incorporated into security mitigations including for glazing systems. (K51, K52, S27)	
Technical Security K30 K31 K32 K33 K34 K35 K36 S18 S19	Applies principles of technical security and information egress covering all elements of technical surveillance to existing protective security measures when developing mitigations against technical attack vectors. (K30, K31, K32, K33, K35, K36, S19) Develops converged mitigations to mitigate technical attack vectors. (K34, S18)	Substantiates how recommended mitigations for technical attack vectors improve existing protective security. (K33, S19)
Threat Management K11 K12 K13 S9 B3	Develops threat analysis reviews using information	Analyse used sources and types of information and

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
	sources, in a timely manner based on an organisation's assets, services and location, applying asset identification and classification principles. (K11, K12, K13, S9, B3)	the effect these have on applying classification principles in the production of a threat analysis. (K12, S9)

Professional discussion underpinned by a portfolio of evidence

Fail - does not meet pass criteria

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
Analysis K50 K53 K56 S26 S28 S31	Explains how they adapt to changing environments, utilising organisational learning and problem-solving tools to influence organisational protective security design and resilience. (K50, K56, S26, S31) Explains how reflective practice, feedback and professional development activities have enhanced their approach to operational activities and enhances protective security resilience. (K53, S28)	Evaluates the concept of organisational resilience and learning and how these impact the use of logical thinking and use of problem-solving tools. (K50, S30)
Communication K9 K55 K58 S7 S30 S33 B4	Describes the challenges faced by individuals from different social-economic and diverse backgrounds and how	Evaluates how organisational reporting protocols can affect decision making during investigations. (K58, S33)

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
	they provide support to these individuals. (K9, S7, B4) Explains how their assessment of information gained through digital technology has supported decision making and how they comply with organisational reporting protocols. (K55, K58, S30, S33)	
Legislation K5 S3	Explains how they applied legislation, local and national policies and practice when creating mitigations and how this was applied within limits of own role. (K5, S3)	None.
Governance K6 K7 K49 S4 S5 S25	Explains how they interpret organisational need and objectives and consider return on investment and perform cost benefit analysis of differing security approaches to create recommendations, utilising the governance process to influence senior leadership. (K6, K7, K49, S4, S5, S25)	Evaluates how they have engaged and influenced the governance process and how this has the impacted on protective security risk decisions. (K6, K7, S4, S5)
Response Management K47 K48 S23 S24 B2	Explains how their Incident Response and Incident Management plans contribute to efficiency and	Evaluates the efficiency of their incident response plans, incident management plans and information gathered for

THEME KSBS	PASS APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS	DISTINCTION APPRENTICES MUST DEMONSTRATE ALL OF THE PASS DESCRIPTORS AND ALL OF THE DISTINCTION DESCRIPTORS
	organisational resilience. (K47, S23) Independently gathers, grades and reviews information as part of an investigation, to make recommendations for decision making. (K48, S24, B2)	investigations. K47, K48, S23, S24)
Standards K8 S6	Explains the implications of non-compliance of ISO standards within limits of own role. (K8, S6)	None.
Personal Security K29 S17	Explains how they demonstrate personal security and safety protocols in the work environment. (K29, S17)	None.

Overall EPA grading

Performance in the EPA determines the overall grade of:

- fail
- pass
- merit
- distinction

An independent assessor must individually grade the project report with presentation and professional discussion underpinned by a portfolio of evidence in line with this EPA plan. The EPAO must combine the individual assessment method grades to determine the overall EPA grade.

If the apprentice fails one assessment method or more, they will be awarded an overall fail.

To achieve an overall pass, the apprentice must achieve at least a pass in all the assessment methods. For the apprentice to achieve an overall distinction grade they will need to achieve distinction in both assessment methods.
Grades from individual assessment methods must be combined in the following way to determine the grade of the EPA overall.

PROJECT REPORT WITH PRESENTATION	PROFESSIONAL DISCUSSION UNDERPINNED BY A PORTFOLIO OF EVIDENCE	OVERALL GRADING
Any grade	Fail	Fail
Fail	Any grade	Fail
Pass	Pass	Pass
Pass	Distinction	Merit
Distinction	Pass	Merit
Distinction	Distinction	Distinction

Re-sits and re-takes

If the apprentice fails one assessment method or more, they can take a re-sit or a re-take at their employer's discretion. The apprentice's employer needs to agree that a re-sit or re-take is appropriate. A re-sit does not need further learning, whereas a re-take does. The apprentice should have a supportive action plan to prepare for a re-sit or a re-take.

The employer and the EPAO should agree the timescale for a re-sit or re-take. A re-sit is typically taken within 2 months of the EPA outcome notification. The timescale for a re-take is dependent on how much re-training is required and is typically taken within 3 months of the EPA outcome notification.
If the apprentice fails the project assessment method, they must amend the project output in line with the independent assessor's feedback. The apprentice will be given 2 weeks to rework and submit the amended report.
Failed assessment methods must be re-sat or re-taken within a 6-month period from the EPA outcome notification, otherwise the entire EPA will need to be re-sat or re-taken in full.

Re-sits and re-takes are not offered to an apprentice wishing to move from pass to a higher grade.

The apprentice will get a maximum EPA grade of pass if they need to re-sit or re-take one or more assessment methods, unless the EPAO determines there are exceptional circumstances.

Roles and responsibilities

ROLES	RESPONSIBILITIES
Apprentice	As a minimum, the apprentice should: • complete on-programme training to meet the KSBs as outlined in the apprenticeship standard for a minimum of 12 months • complete the required amount of off-the-job training specified by the apprenticeship funding rules and as arranged by the employer and training provider • understand the purpose and importance of EPA • prepare for and undertake the EPA including meeting all gateway requirements
Employer	As a minimum, the apprentice's employer must: • select the training provider • work with the training provider to select the EPAO • work with the training provider, where applicable, to support the apprentice in the workplace and to provide the opportunities for the apprentice to develop the KSBs • arrange and support off-the-job training to be undertaken by the apprentice • decide when the apprentice is working at or above the apprenticeship standard and is ready for EPA • ensure the apprentice is prepared for the EPA • ensure that all supporting evidence required at the gateway is submitted in line with this EPA plan • confirm arrangements with the EPAO for the EPA in a timely manner, including who, when, where • provide the EPAO with access to any employer-specific documentation as required for example, company policies • ensure that the EPA is scheduled with the EPAO for a date and time which allows appropriate opportunity for the apprentice to meet the KSBs • ensure the apprentice is given sufficient time away from regular duties to prepare for, and complete the EPA

ROLES	RESPONSIBILITIES
	• ensure that any required supervision during the EPA period, as stated within this EPA plan, is in place • ensure the apprentice has access to the resources used to fulfil their role and carry out the EPA for workplace based assessments • remain independent from the delivery of the EPA • pass the certificate to the apprentice upon receipt
EPAO	As a minimum, the EPAO must: • conform to the requirements of this EPA plan and deliver its requirements in a timely manner • conform to the requirements of the apprenticeship provider and assessment register • conform to the requirements of the external quality assurance provider (EQAP) • understand the apprenticeship including the occupational standard and EPA plan • make all necessary contractual arrangements including agreeing the price of the EPA • develop and produce assessment materials including specifications and marking materials, for example mark schemes, practice materials, training material • maintain and apply a policy for the declaration and management of conflict of interests and independence. This must ensure, as a minimum, there is no personal benefit or detriment for those delivering the EPA or from the result of an assessment. It must cover: o apprentices o employers o independent assessors o any other roles involved in delivery or grading of the EPA • have quality assurance systems and procedures that ensure fair, reliable and consistent assessment and maintain records of internal quality assurance (IQA) activity for external quality assurance (EQA) purposes • appoint independent, competent, and suitably qualified assessors in line with the requirements of this EPA plan

ROLES	RESPONSIBILITIES
	• appoint administrators, invigilators and any other roles where required to facilitate the EPA • deliver induction, initial and on-going training for all their independent assessors and any other roles involved in the delivery or grading of the EPA as specified within this EPA plan. This should include how to record the rationale and evidence for grading decisions where required • conduct standardisation with all their independent assessors before allowing them to deliver an EPA, when the EPA is updated, and at least once a year • conduct moderation across all of their independent assessors' decisions once EPAs have started according to a sampling plan, with associated risk rating of independent assessors • monitor the performance of all their independent assessors and provide additional training where necessary • develop and provide assessment recording documentation to ensure a clear and auditable process is in place for providing assessment decisions and feedback to all relevant stakeholders • use language in the development and delivery of the EPA that is appropriate to the level of the apprenticeship • arrange for the EPA to take place in a timely manner, in consultation with the employer • provide information, advice, and guidance documentation to enable apprentices, employers and training providers to prepare for the EPA • confirm the gateway requirements have been met before they start the EPA for an apprentice • arrange a suitable venue for the EPA • maintain the security of the EPA including, but not limited to, verifying the identity of the apprentice, invigilation and security of materials • where the EPA plan permits assessment away from the workplace, ensure that the apprentice has access to the required resources and liaise with the employer to agree this if necessary • confirm the overall grade awarded • maintain and apply a policy for conducting appeals

ROLES	RESPONSIBILITIES
Independent assessor	As a minimum, an independent assessor must: • be independent, with no conflict of interest with the apprentice, their employer or training provider, specifically, they must not receive a personal benefit or detriment from the result of the assessment • have, maintain and be able to evidence up-to-date knowledge and expertise of the occupation • have the competence to assess the EPA and meet the requirements of the IQA section of this EPA plan • understand the apprenticeship's occupational standard and EPA plan • attend induction and standardisation events before they conduct an EPA for the first time, when the EPA is updated, and at least once a year • use language in the delivery of the EPA that is appropriate to the level of the apprenticeship • work with other personnel, where used, in the preparation and delivery of assessment methods • conduct the EPA to assess the apprentice against the KSBs and in line with the EPA plan • make final grading decisions in line with this EPA plan • record and report assessment outcome decisions • comply with the IQA requirements of the EPAO • comply with external quality assurance (EQA) requirements
Training provider	As a minimum, the training provider must: • conform to the requirements of the apprenticeship provider and assessment register • ensure procedures are in place to mitigate against any conflict of interest • work with the employer and support the apprentice during the off-the-job training to provide the opportunities to develop the KSBs as outlined in the occupational standard • deliver training to the apprentice as outlined in their apprenticeship agreement • monitor the apprentice's progress during any training provider led on-programme learning

ROLES	RESPONSIBILITIES
	• ensure the apprentice is prepared for the EPA • work with the employer to select the EPAO • advise the employer, upon request, on the apprentice's readiness for EPA • ensure that all supporting evidence required at the gateway is submitted in line with this EPA plan • remain independent from the delivery of the EPA

Reasonable adjustments

Reasonable adjustments
The EPAO must have reasonable adjustments arrangements for the EPA.

This should include:

- how an apprentice qualifies for a reasonable adjustment
- what reasonable adjustments may be made

Adjustments must maintain the validity, reliability and integrity of the EPA as outlined in this EPA plan.

Special considerations
The EPAO must have special consideration arrangements for the EPA.

This should include:

- how an apprentice qualifies for a special consideration
- what special considerations will be given

Special considerations must maintain the validity, reliability and integrity of the EPA as outlined in this EPA plan.

Internal quality assurance

Internal quality assurance refers to the strategies, policies and procedures that an EPAO must have in place to ensure valid, consistent and reliable EPA decisions.

EPAOs for this EPA must adhere to the requirements within the roles and responsibilities table.

They must also appoint independent assessors who:

- have recent relevant experience of the occupation or sector to at least occupational level 2 gained in the last 3 years or significant experience of the occupation or sector
- have professional body membership with:

    - Chartered Security Professional (CSyP)
    - Register of Security Engineering Specialists (RSES) or hold a relevant masters in security risk management
- meet the following minimum requirements:
  qualified, or working towards an assessor qualification

Value for money

Affordability of the EPA will be aided by using at least some of the following:

- utilising digital remote platforms to conduct applicable assessment methods
- using the employer's premises
- conducting assessment methods on the same day

Professional recognition

This apprenticeship is not aligned to professional recognition.

Mapping of KSBs to assessment methods

KNOWLEDGE	ASSESSMENT METHODS
K1 Crime and security science theories and how they underpin protective security design to provide a layered security approach and why security matters to protect businesses and society: Routine Activity Theory, Rational Choice Theory, Offender Typologies, Crime Mapping, Broken Windows Theory, the security triangle of detection, response and delay, Situational Crime Prevention, Social Crime Prevention, adversary path analysis, Crime Prevention through Environmental Design and Defence in depth based on National Protective Security Authority (NPSA) deter, detect, delay, mitigate, respond principles.	Project report with presentation
K2 The protective security eco-system, the role played by key organisations and how each National Technical Authority (NTAs) contributes to the protective security of business and society: the Register of Security Engineering Specialists (RSES) and Chartered Security Professionals (CSyP).	Project report with presentation
K3 How the security convergence of the four main disciplines of protective services Cyber, Personnel, Physical and Technical can mitigate vulnerabilities of the siloed approach to security risk management.	Project report with presentation
K4 Importance of a single overview of risk for senior risk owners by employing security convergence.	Project report with presentation
K5 The main features and how to apply significant law to individual organisations: the Occupiers Liability, Health and Safety, Management of Health and Safety at Work Regulations, Fire Safety, Data Protection, the National Security Act, the	Professional discussion underpinned by a portfolio of evidence

KNOWLEDGE	ASSESSMENT METHODS
National Security Investment Act, the Security Services Act, Common Law and Criminal Law, the Digital Online Resilience Act, UK AI Act, Communications Act, Computer Misuse Act, Data Protection Act, GDPR, Network and Information Systems Regulations, Privacy and Electronic Communications Regulation.	
K6 Principles of good governance, governance structure and protective security oversight of cyber, physical, personnel and technical security including two-way communication channels, security risk registers, an accountable board level risk owner and structure for dissemination of information and decisions.	Professional discussion underpinned by a portfolio of evidence
K7 The influence of organisational objectives and differing protective security approaches taken in the context of government, Critical National Infrastructure, multi-nationals, academia, start-ups and emerging technology.	Professional discussion underpinned by a portfolio of evidence
K8 The requirements of ISO standards and their application in protective security.	Professional discussion underpinned by a portfolio of evidence
K9 The challenges faced by individuals from diverse backgrounds, with differing social-economic and societal perceptions when seeking and interacting with colleagues and stakeholders.	Professional discussion underpinned by a portfolio of evidence
K10 Principles of asset identification and classification: physical, information, people assets and anything that enables a business to operate e.g. a process, system, document or person and brand and reputation.	Project report with presentation
K11 The influence of intent and capability on threat actor actions.	Project report with presentation
K12 Information sources and the types of information of potential threats to security: the National Protective Security Authority (NPSA), National Cyber Security Centre (NCSC), UK National Authority for Counter Eavesdropping (UK NACE), National Counter Terror Security Office (NaCTSO), MI5, Police, local crime statistics and external stakeholders.	Project report with presentation
K13 Threat Intelligence Cycle and how to use threat assessments to conduct threat analysis based on a range of threat scenarios that organisations would potentially face based on their assets, services provided and locations.	Project report with presentation
K14 Principles of security risk management including how threat, vulnerability and impact determines the risk posed to an organisation, its assets and people and how mitigating threat, vulnerabilities and impact can be supported with protective security.	Project report with presentation

KNOWLEDGE	ASSESSMENT METHODS
K15 The principles of quantitative, qualitative and semi-qualitative risk assessment methodologies to develop risk statements including threat actors, assets targeted, attack vectors used, and potential impact aligned to organisational assets, threat, vulnerability and impact.	Project report with presentation
K16 The concepts, main functions and benefits of security risk registers for governance, mitigations, risk tolerance and corporate memory and how they support the production of Operational Requirements.	Project report with presentation
K17 Common security standards to mitigate forcible attack vectors including Loss Prevention Standards (LPS) 1673, LPS 1178 Issue 8, NPSA Marauding Terrorist Attack Standard and NPSA Manual Forced Entry Standards (MFES).	Project report with presentation
K18 The main types of postal/courier attack vectors and mitigations and the principles of the PAS 97: 2021 Mail Screening and Security-Specification.	Project report with presentation
K19 The main types of glazing specification, glazing systems vulnerabilities and mitigation against forcible attack and blast.	Project report with presentation
K20 NPSA principles on threats to security posed by vehicles: Vehicle as a Weapon (VAW), Vehicle Borne Improvised Explosive Device (VBIED) and the Layered Vehicle Attack and the potential risk they provide to organisations, businesses and society and how ISO 22343-1: 2023 Vehicle security barriers supports building resilience for security threats with Hostile Vehicle Mitigation strategies.	Project report with presentation
K21 Methodology used by threat actors during marauding terrorist attacks and NPSA recommended measures to minimise the impact of Marauding Terrorist Attack to save lives.	Project report with presentation
K22 Principles of the NPSA Surreptitious Threat Mitigation Process (STaMP) employing NPSA Surreptitious Attack Protective Security Philosophy.	Project report with presentation
K23 Principles of the Cyber Assurance Physical Security Systems (CAPSS).	Project report with presentation
K24 Governmental, Independent and third-party certification of physical security products and standards e.g. NPSA Catalogue of Security Equipment (CSE), Redbook LIVE.	Project report with presentation
K25 How organisations can manage potential insider threat, insider risk and insider events: leadership, governance, pre-employment screening and vetting, ongoing personnel security, employee monitoring and assessment, investigation and disciplinary practices, an security culture with security focused behaviour embedding NPSA's 5 Es, effective and line management, organisational insider threat stakeholder group	Project report with presentation

KNOWLEDGE	ASSESSMENT METHODS
utilising the NPSA ten steps of insider risk assessment and isomorphic learning.	
K26 How the threat landscape and societal challenges influence motivations and methods used by insiders and insider event typologies: unauthorised disclosure of sensitive information, process corruption, unauthorised provision of third-party access to organisational assets, financial gain through financial corruption and workplace violence.	Project report with presentation
K27 The integration of personnel, cyber, physical and technical security controls to mitigate insider risk.	Project report with presentation
K28 Principles of hostile reconnaissance and hostile planning stages, and how protective security can be used to disrupt hostile reconnaissance employing the principles of NPSA DENY, DETECT and DETER strategy and the integration of Security Minded Communications, See Check and Notify (SCaN) and Project Servator.	Project report with presentation
K29 The role individuals can play to ensure their personal security and safety when working for an organisation: personal situational awareness, online vigilance, maintain residential security, planning prior to travel, managing own digital footprint, protect sensitive information, follow organisational personal security emergency procedures.	Professional discussion underpinned by a portfolio of evidence
K30 The principles of technical security and why and how organisations may be targeted.	Project report with presentation
K31 The required elements of a technical surveillance device.	Project report with presentation
K32 The principles of information egress via spatial, physical and conductive methods used during standoff and close access technical collection operations.	Project report with presentation
K33 How existing protective security may encourage threat actors to employ technical attack vectors.	Project report with presentation
K34 The convergence of physical, personnel and people security to mitigate standoff attacks and close access technical collection operations.	Project report with presentation
K35 The technical security attack vectors: overt access of visitors and contractors, commercial off the shelf 'quick plant' products, human interface devices, mobile telephones, smart devices, long lensing, drones, laser microphones and deep plant devices, 'man-in-the-middle', Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) attacks, and lip-reading attack vectors.	Project report with presentation
K36 How to mitigate against technical attacks during 'overt access': quick plant devices, human interface devices, remote	Project report with presentation

KNOWLEDGE	ASSESSMENT METHODS
access trojans, international mobile subscriber Identification catchers, man-in-the-middle, vulnerabilities created by smart devices, long lensing, lip reading, drones, laser microphones and deep plants.	
K37 The concept and applicability of Confidentiality, Integrity and Availability (CIA) for cyber security.	Project report with presentation
K38 The main features of malware and how they can get into a computer via human and technical factors.	Project report with presentation
K39 The threat vectors used by threat actor and mitigations: phishing, spam, spoofing, click-fraud and botnets and attacks on 'End of Life' software, anti-virus software, sandboxes and code-signing.	Project report with presentation
K40 The principles of how the internet works including Transmission Control Protocol (TCP), Internet Protocol (IP), how datagrams, packets work, and the principles of wireless Local Access Networks.	Project report with presentation
K41 The methods employed by threat actors to gain data including employing Wi-Fi hotspots, packet sniffing and man-in-the middle attacks.	Project report with presentation
K42 The principles of encryption, cryptography, asymmetric cryptography, encryption keys, secure web browsing, and methods to protect data on the network.	Project report with presentation
K43 The vulnerabilities of short encryption keys, and the Network Intrusion Detection Systems and Host Intruder Detection Systems.	Project report with presentation
K44 The consequences of common network security threats and insider threats on data loss: recreating lost data, purchasing new hardware, purchasing new software, cost of continuing without the available data, the cost involved with informing others of the data loss.	Project report with presentation
K45 How cyber security supports authentication and access to organisational systems including good password practice, salting in collaboration with hashing, use of hardware tokens.	Project report with presentation
K46 Attack vectors used including hashes and brute force attack.	Project report with presentation
K47 The principles of incident response and incident management.	Professional discussion underpinned by a portfolio of evidence
K48 The principles of investigation for security incidents including gathering and grading information to be used in investigations, processing information and making recommendations for decision making.	Professional discussion underpinned by a portfolio of evidence

KNOWLEDGE	ASSESSMENT METHODS
K49 The principles of a Return on Security Investment (ROSI) and cost benefit analysis and its alignment with organisational aims and objectives and impact on security decision making.	Professional discussion underpinned by a portfolio of evidence
K50 The concept of organisational resilience and learning and its interdependency with protective security to enable organisational resilience in a changing environment.	Professional discussion underpinned by a portfolio of evidence
K51 The principles to promote sustainable working practices in protective security.	Project report with presentation
K52 How glazing systems can impact the carbon footprint of buildings: laminated glass, annealed/float glass, tough/tempered glass, heat strengthened glass, laminated glass sandwich and polycarbonate.	Project report with presentation
K53 The use of reflective practice theories and techniques to inform professional development of an individual and improve approaches to own practice and operational activities.	Professional discussion underpinned by a portfolio of evidence
K54 Techniques for managing challenging communications using language and style that reflect the situation and audience.	Project report with presentation
K55 The use of digital technology to support investigations and assist decision making.	Professional discussion underpinned by a portfolio of evidence
K56 Problem solving tools and techniques.	Professional discussion underpinned by a portfolio of evidence
K57 Principles of influencing techniques to achieve goals and objectives.	Project report with presentation
K58 Methods for reporting, in accordance with organisational procedure.	Professional discussion underpinned by a portfolio of evidence
K59 Presentation methods for different audiences using communication skills and strategies to maximise understanding of intended purpose.	Project report with presentation
SKILL	**ASSESSMENT METHODS**
S1 Utilise crime and security science knowledge and theory in the planning of organisational protective security to address protective security requirements and meet organisational needs.	Project report with presentation
S2 Apply the principles of security convergence to protective security planning.	Project report with presentation
S3 Comply with legislation, local and national policies and practice within limits of own role.	Professional discussion underpinned by a portfolio of evidence

KNOWLEDGE	ASSESSMENT METHODS
S4 Engage and influence the governance process to enable security risk decisions.	Professional discussion underpinned by a portfolio of evidence
S5 Interpret organisational needs in the application of protective security.	Professional discussion underpinned by a portfolio of evidence
S6 Follow ISO standards within limits of own role with consideration of the implications of non-compliance.	Professional discussion underpinned by a portfolio of evidence
S7 Support individuals with differing social-economic and diverse backgrounds who are faced with challenges when interacting with colleagues and stakeholders.	Professional discussion underpinned by a portfolio of evidence
S8 Produce asset registers for organisations, applying asset identification and classification principles.	Project report with presentation
S9 Produce 'Threat Analysis' based on an organisation's assets, services and location, applying asset identification and classification principles.	Project report with presentation
S10 Assess vulnerability and impact to the organisation within protective security risk documentation.	Project report with presentation
S11 Produce a security risk assessment.	Project report with presentation
S12 Develop physical security mitigations for forcible attack vectors.	Project report with presentation
S13 Develop physical security mitigations for surreptitious attack vectors.	Project report with presentation
S14 Utilise assured products to mitigate protective security risk.	Project report with presentation
S15 Develop measures to mitigate against organisational insider risk.	Project report with presentation
S16 Develop mitigations against hostile reconnaissance.	Project report with presentation
S17 Apply personal security and safety protocols in the work environment.	Professional discussion underpinned by a portfolio of evidence
S18 Develop mitigations, using converged security, to mitigate technical security attack vectors.	Project report with presentation
S19 Develop mitigations for technical security attack vectors.	Project report with presentation

KNOWLEDGE	ASSESSMENT METHODS
S20 Review identified vulnerabilities that could be exploited by malware in organisational assets to develop mitigations to protect confidentiality, integrity and availability of data.	Project report with presentation
S21 Develop mitigations to prevent data loss within organisations.	Project report with presentation
S22 Utilise organisational cyber security approaches for authentication and access with full consideration of password good practise mitigations and for potential attack vectors.	Project report with presentation
S23 Review Incident Response and Incident Management plans to ensure efficiency contributing to organisational resilience.	Professional discussion underpinned by a portfolio of evidence
S24 Review information gathered through investigations to make recommendations for decision making.	Professional discussion underpinned by a portfolio of evidence
S25 Make recommendations to senior leadership for protective security.	Professional discussion underpinned by a portfolio of evidence
S26 Utilise organisational learning to enhance protective security and resilience.	Professional discussion underpinned by a portfolio of evidence
S27 Incorporate sustainable practise when designing security mitigations.	Project report with presentation
S28 Engage in self-reflection, feedback and professional development activities to improve own professional practice.	Professional discussion underpinned by a portfolio of evidence
S29 Manage challenging communications using language and style that reflect the situation and audience.	Project report with presentation
S30 Assess information gained through digital technology to inform decisions.	Professional discussion underpinned by a portfolio of evidence
S31 Apply logical thinking and problem-solving tools and techniques, identifying issues and proposing solutions to problems.	Professional discussion underpinned by a portfolio of evidence
S32 Apply influencing techniques to achieve goals and objectives.	Project report with presentation
S33 Follow organisational reporting protocols.	Professional discussion underpinned by a portfolio of evidence
S34 Create and deliver presentations using communication skills and strategies to maximise understanding of intended purpose.	Project report with presentation

BEHAVIOUR	ASSESSMENT METHODS
B1 Committed to supporting a strong security posture.	Project report with presentation
B2 Works independently and takes responsibility working diligently regardless of supervision levels.	Professional discussion underpinned by a portfolio of evidence
B3 Effective time management.	Project report with presentation
B4 Embraces Equality, Diversity and Inclusion treating everyone with dignity and respect.	Professional discussion underpinned by a portfolio of evidence

Mapping of KSBs to grade themes

Project report with presentation

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
Communication K54 K57 K59 S29 S32 S34	Techniques for managing challenging communications using language and style that reflect the situation and audience. (K54) Principles of influencing techniques to achieve goals and objectives. (K57) Presentation methods for different audiences using communication skills and strategies to maximise understanding of intended purpose. (K59)	Manage challenging communications using language and style that reflect the situation and audience. (S29) Apply influencing techniques to achieve goals and objectives. (S32) Create and deliver presentations using communication skills and strategies to maximise understanding of intended purpose. (S34)	None
Cyber Security K37 K38 K39 K40 K41 K42 K43 K44 K45 K46 S20 S21 S22	The concept and applicability of Confidentiality, Integrity and Availability (CIA) for cyber security. (K37) The main features of malware and how they can get into a	Review identified vulnerabilities that could be exploited by malware in organisational assets to develop mitigations to protect	None

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	computer via human and technical factors. (K38) The threat vectors used by threat actor and mitigations: phishing, spam, spoofing, click-fraud and botnets and attacks on 'End of Life' software, anti-virus software, sandboxes and code-signing. (K39) The principles of how the internet works including Transmission Control Protocol (TCP), Internet Protocol (IP), how datagrams, packets work, and the principles of wireless Local Access Networks. (K40) The methods employed by threat actors to gain data including employing Wi-Fi hotspots, packet sniffing and man-in-the middle attacks. (K41) The principles of encryption, cryptography, asymmetric cryptography, encryption keys, secure web browsing, and methods to protect data on the network. (K42) The vulnerabilities of short encryption keys, and the Network Intrusion Detection Systems and Host Intruder Detection Systems. (K43) The consequences of common network security threats and insider threats on data loss: recreating lost data, purchasing new hardware, purchasing new software, cost of continuing without the available data, the cost involved with informing others of the data loss. (K44)	confidentiality, integrity and availability of data. (S20) Develop mitigations to prevent data loss within organisations. (S21) Utilise organisational cyber security approaches for authentication and access with full consideration of password good practise mitigations and for potential attack vectors. (S22)	

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	How cyber security supports authentication and access to organisational systems including good password practice, salting in collaboration with hashing, use of hardware tokens. (K45) Attack vectors used including hashes and brute force attack. (K46)		
People Security K28 S16 B1	Principles of hostile reconnaissance and hostile planning stages, and how protective security can be used to disrupt hostile reconnaissance employing the principles of NPSA DENY, DETECT and DETER strategy and the integration of Security Minded Communications, See Check and Notify (SCaN) and Project Servator. (K28)	Develop mitigations against hostile reconnaissance. (S16)	Committed to supporting a strong security posture. (B1)
Personnel Security K25 K26 K27 S15	How organisations can manage potential insider threat, insider risk and insider events: leadership, governance, pre-employment screening and vetting, ongoing personnel security, employee monitoring and assessment, investigation and disciplinary practices, an security culture with security focused behaviour embedding NPSA's 5 Es, effective and line management, organisational insider threat stakeholder group utilising the NPSA ten steps of insider risk assessment and isomorphic learning. (K25) How the threat landscape and societal challenges influence motivations and methods used by insiders and insider event typologies: unauthorised	Develop measures to mitigate against organisational insider risk. (S15)	None

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	disclosure of sensitive information, process corruption, unauthorised provision of third-party access to organisational assets, financial gain through financial corruption and workplace violence. (K26) The integration of personnel, cyber, physical and technical security controls to mitigate insider risk. (K27)		
Physical Security K17 K18 K19 K20 K21 K22 K23 K24 S12 S13 S14	Common security standards to mitigate forcible attack vectors including Loss Prevention Standards (LPS) 1673, LPS 1178 Issue 8, NPSA Marauding Terrorist Attack Standard and NPSA Manual Forced Entry Standards (MFES). (K17) The main types of postal/courier attack vectors and mitigations and the principles of the PAS 97: 2021 Mail Screening and Security-Specification. (K18) The main types of glazing specification, glazing systems vulnerabilities and mitigation against forcible attack and blast. (K19) NPSA principles on threats to security posed by vehicles: Vehicle as a Weapon (VAW), Vehicle Borne Improvised Explosive Device (VBIED) and the Layered Vehicle Attack and the potential risk they provide to organisations, businesses and society and how ISO 22343-1: 2023 Vehicle security barriers supports building resilience for security threats	Develop physical security mitigations for forcible attack vectors. (S12) Develop physical security mitigations for surreptitious attack vectors. (S13) Utilise assured products to mitigate protective security risk. (S14)	None

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	with Hostile Vehicle Mitigation strategies. (K20) Methodology used by threat actors during marauding terrorist attacks and NPSA recommended measures to minimise the impact of Marauding Terrorist Attack to save lives. (K21) Principles of the NPSA Surreptitious Threat Mitigation Process (STaMP) employing NPSA Surreptitious Attack Protective Security Philosophy. (K22) Principles of the Cyber Assurance Physical Security Systems (CAPSS). (K23) Governmental, Independent and third-party certification of physical security products and standards e.g. NPSA Catalogue of Security Equipment (CSE), Redbook LIVE. (K24)		
Risk Management K1 K2 K3 K4 K10 K14 K15 K16 K51 K52 S1 S2 S8 S10 S11 S27	Crime and security science theories and how they underpin protective security design to provide a layered security approach and why security matters to protect businesses and society: Routine Activity Theory, Rational Choice Theory, Offender Typologies, Crime Mapping, Broken Windows Theory, the security triangle of detection, response and delay, Situational Crime Prevention, Social Crime Prevention, adversary path analysis, Crime Prevention through Environmental Design and Defence in depth based on National Protective Security	Utilise crime and security science knowledge and theory in the planning of organisational protective security to address protective security requirements and meet organisational needs. (S1) Apply the principles of security convergence to protective security planning. (S2) Produce asset registers for organisations,	None

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	Authority (NPSA) deter, detect, delay, mitigate, respond principles. (K1) The protective security eco-system, the role played by key organisations and how each National Technical Authority (NTAs) contributes to the protective security of business and society: the Register of Security Engineering Specialists (RSES) and Chartered Security Professionals (CSyP). (K2) How the security convergence of the four main disciplines of protective services Cyber, Personnel, Physical and Technical can mitigate vulnerabilities of the siloed approach to security risk management. (K3) Importance of a single overview of risk for senior risk owners by employing security convergence. (K4) Principles of asset identification and classification: physical, information, people assets and anything that enables a business to operate e.g. a process, system, document or person and brand and reputation. (K10) Principles of security risk management including how threat, vulnerability and impact determines the risk posed to an organisation, its assets and people and how mitigating threat, vulnerabilities and impact can be supported with protective security. (K14)	applying asset identification and classification principles. (S8) Assess vulnerability and impact to the organisation within protective security risk documentation. (S10) Produce a security risk assessment. (S11) Incorporate sustainable practise when designing security mitigations. (S27)	

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	The principles of quantitative, qualitative and semi-qualitative risk assessment methodologies to develop risk statements including threat actors, assets targeted, attack vectors used, and potential impact aligned to organisational assets, threat, vulnerability and impact. (K15) The concepts, main functions and benefits of security risk registers for governance, mitigations, risk tolerance and corporate memory and how they support the production of Operational Requirements. (K16) The principles to promote sustainable working practices in protective security. (K51) How glazing systems can impact the carbon footprint of buildings: laminated glass, annealed/float glass, tough/tempered glass, heat strengthened glass, laminated glass sandwich and polycarbonate. (K52)		
Technical Security K30 K31 K32 K33 K34 K35 K36 S18 S19	The principles of technical security and why and how organisations may be targeted. (K30) The required elements of a technical surveillance device. (K31) The principles of information egress via spatial, physical and conductive methods used during standoff and close access technical collection operations. (K32)	Develop mitigations, using converged security, to mitigate technical security attack vectors. (S18) Develop mitigations for technical security attack vectors. (S19)	None

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	How existing protective security may encourage threat actors to employ technical attack vectors. (K33) The convergence of physical, personnel and people security to mitigate standoff attacks and close access technical collection operations. (K34) The technical security attack vectors: overt access of visitors and contractors, commercial off the shelf 'quick plant' products, human interface devices, mobile telephones, smart devices, long lensing, drones, laser microphones and deep plant devices, 'man-in-the-middle', Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) attacks, and lip-reading attack vectors. (K35) How to mitigate against technical attacks during 'overt access': quick plant devices, human interface devices, remote access trojans, international mobile subscriber Identification catchers, man-in-the-middle, vulnerabilities created by smart devices, long lensing, lip reading, drones, laser microphones and deep plants. (K36)		
Threat Management K11 K12 K13 S9 B3	The influence of intent and capability on threat actor actions. (K11) Information sources and the types of information of potential threats to security: the National Protective Security	Produce 'Threat Analysis' based on an organisation's assets, services and location, applying asset identification and	Effective time management. (B3)

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	Authority (NPSA), National Cyber Security Centre (NCSC), UK National Authority for Counter Eavesdropping (UK NACE), National Counter Terror Security Office (NaCTSO), MI5, Police, local crime statistics and external stakeholders. (K12) Threat Intelligence Cycle and how to use threat assessments to conduct threat analysis based on a range of threat scenarios that organisations would potentially face based on their assets, services provided and locations. (K13)	classification principles. (S9)	

Professional discussion underpinned by a portfolio of evidence

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
Analysis K50 K53 K56 S26 S28 S31	The concept of organisational resilience and learning and its interdependency with protective security to enable organisational resilience in a changing environment. (K50) The use of reflective practice theories and techniques to inform professional development of an individual and improve approaches to own practice and operational activities. (K53) Problem solving tools and techniques. (K56)	Utilise organisational learning to enhance protective security and resilience. (S26) Engage in self-reflection, feedback and professional development activities to improve own professional practice. (S28) Apply logical thinking and problem-solving tools and techniques, identifying issues and proposing solutions to problems. (S31)	None
Communication K9 K55 K58 S7 S30 S33 B4	The challenges faced by individuals from diverse backgrounds, with differing social-economic and societal	Support individuals with differing social-economic and diverse backgrounds who are	Embraces Equality, Diversity and Inclusion treating

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	perceptions when seeking and interacting with colleagues and stakeholders. (K9) The use of digital technology to support investigations and assist decision making. (K55) Methods for reporting, in accordance with organisational procedure. (K58)	faced with challenges when interacting with colleagues and stakeholders. (S7) Assess information gained through digital technology to inform decisions. (S30) Follow organisational reporting protocols. (S33)	everyone with dignity and respect. (B4)
Legislation K5 S3	The main features and how to apply significant law to individual organisations: the Occupiers Liability, Health and Safety, Management of Health and Safety at Work Regulations, Fire Safety, Data Protection, the National Security Act, the National Security Investment Act, the Security Services Act, Common Law and Criminal Law, the Digital Online Resilience Act, UK AI Act, Communications Act, Computer Misuse Act, Data Protection Act, GDPR, Network and Information Systems Regulations, Privacy and Electronic Communications Regulation. (K5)	Comply with legislation, local and national policies and practice within limits of own role. (S3)	None
Governance K6 K7 K49 S4 S5 S25	Principles of good governance, governance structure and protective security oversight of cyber, physical, personnel and technical security including two-way communication channels, security risk registers, an accountable board level risk owner and	Engage and influence the governance process to enable security risk decisions. (S4) Interpret organisational needs in the application of	None

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
	structure for dissemination of information and decisions. (K6) The influence of organisational objectives and differing protective security approaches taken in the context of government, Critical National Infrastructure, multi-nationals, academia, start-ups and emerging technology. (K7) The principles of a Return on Security Investment (ROSI) and cost benefit analysis and its alignment with organisational aims and objectives and impact on security decision making. (K49)	protective security. (S5) Make recommendations to senior leadership for protective security. (S25)	
Response Management K47 K48 S23 S24 B2	The principles of incident response and incident management. (K47) The principles of investigation for security incidents including gathering and grading information to be used in investigations, processing information and making recommendations for decision making. (K48)	Review Incident Response and Incident Management plans to ensure efficiency contributing to organisational resilience. (S23) Review information gathered through investigations to make recommendations for decision making. (S24)	Works independently and takes responsibility working diligently regardless of supervision levels. (B2)
Standards K8 S6	The requirements of ISO standards and their application in protective security. (K8)	Follow ISO standards within limits of own role with consideration of the implications of non-compliance. (S6)	None
Personal Security	The role individuals can play to ensure their personal	Apply personal security and safety	None

KSBS GROUPED BY THEME	KNOWLEDGE	SKILLS	BEHAVIOUR
K29 S17	security and safety when working for an organisation: personal situational awareness, online vigilance, maintain residential security, planning prior to travel, managing own digital footprint, protect sensitive information, follow organisational personal security emergency procedures. (K29)	protocols in the work environment. (S17)	

External quality assurance

Option selected: Ofqual

Involved employers

Protective Security Centre, Linx International Group/Mitie, Canary Wharf Group, Arqiva, Securigroup, British Museum, City of London Police, Ineos UK Limited, Chubb Insurance, Corps Security, Travis Perkins plc, HM Revenues & Customs (HMRC), Department for Business and Trade, Department for Health and Social Care, Northern Ireland Office, Foreign, Commonwealth & Development Office (FCDO) Services, HM Treasury, Nuclear Waste Services, Gallagher Insurance, Department for Work and Pensions, Nuclear Waste Services, Canary Wharf Management Ltd, Dakin Security Services, Department of Health and Social Care, Government Legal Department, North East Regional Special Operations Unit, National Cyber Security Centre, Security Institute, Cabinet Office, National Protective Security Authority (NPSA), National Authority for Counter-Eavesdropping, Training and Development Unit Counter Terrorism, Home Office.