Institute for Apprenticeships & Technical Education

End-point assessment plan for Cyber Security Technologist apprenticeship standard

Apprenticeship standard reference number	Apprenticeship standard level	Integrated end-point assessment
ST0121	4	No

Contents

Introduction and overview 2
EPA summary table 4
Length of end-point assessment period 5
Order of assessment methods 5
Gateway 6
Assessment methods 8
Reasonable adjustments 20
Grading 21
Re-sits and re-takes 31
Roles and responsibilities 32
Internal Quality Assurance (IQA) 36
Affordability 37
Professional body recognition 37
Mapping of knowledge, skills and behaviours (KSBs) 38

Introduction and overview

This document sets out the requirements for end-point assessment (EPA) for the Cyber Security Technologist apprenticeship standard. It is for end-point assessment organisations (EPAOs) who need to know how EPA for this apprenticeship must operate. It will also be of interest to Cyber Security Technologist apprentices, their employers and training providers.

Cyber Security Technologist includes 3 options as follows:

- Option 1 - Cyber Security Engineer
- Option 2 – Cyber Risk Analyst
- Option 3 – Cyber Security Defend and Respond

Full time apprentices will typically spend 24 months on-programme (before the gateway) working towards the occupational standard, with a minimum of 20% off-the-job training. All apprentices must spend a minimum of 12 months on-programme.

The EPA period should only start, and the EPA be arranged, once the employer is satisfied that the apprentice is deemed to be consistently working at or above the level set out in the occupational standard, all of the pre-requisite gateway requirements for EPA have been met and can be evidenced to an EPAO.

For level 3 apprenticeships and above apprentices without English and mathematics at level 2 must achieve level 2 prior to taking their EPA.

The EPA must be completed within an EPA period lasting typically 4 months, after the EPA gateway.

The EPA consists of 4 discrete assessment methods.

The individual assessment methods will have the following grades:

Assessment method 1: Professional discussion underpinned by portfolio

- Fail
- Pass
- Distinction

Assessment method 2: Scenario demonstrations with questioning

- Fail
- Pass
- Distinction

Assessment method 3: Project report

- Fail
- Pass
- Distinction

Assessment Method 4: Knowledge Test

- Fail
- Pass

Performance in the EPA will determine the overall apprenticeship standard grade of:

- Fail
- Pass
- Merit
- Distinction

EPA summary table

On-programme (typically, 24 months)	Training to develop the occupation standard's knowledge, skills and behaviours (KSBs). Working towards English and mathematics Level 2, if required. Compiling a portfolio of evidence.
End-point assessment gateway	Employer is satisfied the apprentice is consistently working at, or above, the level of the occupational standard. Apprentices must have achieved English and mathematics Level 2 Apprentices must submit a portfolio of evidence to underpin the professional discussion (See Gateway section for full details) The project's subject, title and scope will be agreed between the employer and the EPAO at the gateway
End-point assessment (which will typically take 4 months)	Assessment method 1: **Professional discussion underpinned by portfolio** • Fail • Pass • Distinction Assessment method 2: **Scenario demonstrations with questioning** • Fail • Pass • Distinction Assessment method 3: **Project report** • Fail • Pass • Distinction Assessment method 4: **Knowledge Test** • Fail • Pass

Length of end-point assessment period

The EPA will be completed within an EPA period lasting typically of 4 months, starting when the EPAO has confirmed that all gateway requirements have been met.

Order of assessment methods

The assessment methods can be delivered in any order. The result of one assessment method does not need to be known before starting the next.

Gateway

The apprentice should only enter the gateway once the employer is content that the apprentice is working at or above the occupational standard. In making this decision, the employer may take advice from the apprentice's training provider(s), but the decision must ultimately be made solely by the employer.

The EPAO determines when all other gateway requirements have been met, and the EPA period will only commence once the EPAO has confirmed this.

In addition to the employer's confirmation that the apprentice is working at or above the level in the occupational standard, the apprentice must have completed the following gateway requirements prior to beginning EPA:

- Achieved English and mathematics at Level 2.
  For those with an education, health and care plan or a legacy statement, the apprenticeship's English and mathematics minimum requirement is Entry Level 3.
  British Sign Language (BSL) qualifications are an alternative to English qualifications for those who have BSL as their primary language.

For the **professional discussion underpinned by portfolio** the apprentice will be required to submit a portfolio of evidence. The requirements for this are:

- apprentices must compile a portfolio of evidence during the on-programme period of the apprenticeship
- it should contain evidence related to the KSBs that will be assessed by the professional discussion. Each KSB being assessed should be evidenced more than once. Evidence in the portfolio should be presented under the following section headings:
  - Section 1: Cyber security concepts and its importance to business and society (K3)
  - Section 2: Rationale for security objectives (S6)
  - Section 3: Ethical principles, codes of practice, law & regulation (K8, K9)
  - Section 4: Preventing security breaches & continuous improvement (S9, S15)
  - Section 5: Following organisations policies & processes (K6, S7)
  - Section 6: Operation of security management systems & incident response (K7, K15)
- evidence should be mapped against the KSBs assessed by the Professional Discussion (see mapping of 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/records, for example workplace policies/procedures, records
  - witness statements
  - annotated photographs

  - video clips (maximum total duration 5 minutes); the apprentice must always be in view and identifiable
  - This is not a definitive list; other evidence sources are allowed.
- the portfolio should not include 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 must contain a statement from the employer and apprentice confirming this
- the portfolio of evidence must be submitted to the EPAO at the gateway
- the portfolio of evidence can be electronic or paper-based (or a mixture of both).

the portfolio is not directly assessed. It underpins the professional discussion assessment method and therefore should not be marked by the EPAO. EPAOs should review the portfolio of evidence in preparation for the professional discussion but are not required to provide feedback after this review of the portfolio.

For the **scenario demonstrations with questioning** there are no specific requirements.

For the **project report:**

- The EPAO should sign-off the project's subject, title and scope to confirm its suitability prior to the project commencing. Therefore, a project brief must be submitted to the EPAO at the gateway.

- The project brief must scope out the project and should include:
  - a summary of the stages covered by the project
  - an overview of the tasks involved in the project
  - the specific responsibilities and duties assigned to be undertaken by the apprentice

- The project brief is not assessed and should typically be no more than 500 words.

For the **knowledge test** there are no specific requirements.

Assessment methods

Assessment method 1: Professional discussion underpinned by portfolio (This assessment method has 1 component.)

Overview

This assessment will take the form of a professional discussion which must be appropriately structured to draw out the best of the apprentice's competence and cover the KSBs assigned to this assessment method. It will involve questions that will focus on the KSBs mapped to this method of assessment.

The rationale for this assessment method is that a professional discussion allows a two-way dialogue between the apprentice and independent assessor. It is commonplace for Cyber Security Technologists to engage in detailed technical discussions, so this assessment method mirrors their day to day work.

A professional discussion is a well-recognised method of assessment which is widely used within the digital sector. It allows for knowledge, skills and behaviours that may not naturally occur as part of another assessment method to be assessed and more easily discussed. The apprentice can draw upon other supporting evidence in the portfolio and can effectively determine the authenticity of that supporting evidence.

After the gateway, the EPAO will send the portfolio to the independent assessor a minimum of 10 days before the intended date of the Professional Discussion to allow the independent assessor to review the portfolio and generate appropriate questions.

Delivery

The independent assessor will conduct and assess the professional discussion as set out below.

The professional discussion must last 90 minutes. The independent assessor has the discretion to increase the time of the professional discussion by up to 10% to allow the apprentice to complete their last answer.

During this method, the independent assessor is responsible for generating suitable questions in line with the EPAO's training and standardisation process and using an EPAO question bank as a source of reference.

The independent assessor must ask a minimum of 12 open questions that include at least 2 questions focused on 'law & regulation' (K8) and 1 question on 'ethics' (K9). Follow up questions are permitted where clarity is required.

The independent assessor must use the assessment tools and procedures that are set by the EPAO to record the professional discussion.

The apprentice and the independent assessor will have access to their own copies of the portfolio (either electronic or bring a copy with them) throughout the discussion and both can

refer to it as needed. The apprentice should retain a copy of their portfolio to bring with them to the professional discussion. The apprentice should draw on the contents of the portfolio to underpin the discussion, selecting items to inform and enhance their answers.

The independent assessor must ensure the apprentice has been given the opportunity to evidence all the knowledge, skills and behaviours for the assessment method.

The professional discussion will be graded fail, pass or distinction. The portfolio supports the professional discussion and will not be assessed or graded during the end-point assessment. The independent assessor must allocate grades using the grading criteria.

The independent assessor will make all grading decisions.

Venue

The professional discussion should take place in a quiet room, free from distractions and influence.

The professional discussion can take place in any of the following:

- employer's premises
- a suitable venue selected by the EPAO (for example a training provider's premises)
- online via video conferencing or live streaming.

The professional discussion may be conducted face-to-face or via an electronic platform e.g. video conferencing. EPAOs must ensure appropriate methods to prevent misrepresentation are in place and ensure the apprentice is not being aided in any way should an electronic option be used.

Other relevant information

The EPAO must have in place a system to ensure the quality, currency, consistency and fairness of questions asked by the independent assessors and to prevent predictability from the perspective of the apprentice being assessed. Questions relating to the underpinning KSBs, must be varied yet allow assessment of the relevant KSBs.

EPAOs must ensure that apprentices have a different set of questions in the case of re-sits/re-takes.

Independent assessors must be developed and trained by the EPAO in the conduct of professional discussions and reaching consistent judgement.

EPAOs will produce the following material to support this assessment method:

- outline of the assessment method's requirements
- marking materials
- guidance document for employers and apprentices on the process/timescales for the professional discussion as well as a description of the purpose
- guidance document for independent assessors on how to carry out the assessment

Assessment method 2: Scenario demonstrations with questioning

(This assessment method has 2 components.)

Assessment method 2 component 1: Scenario demonstrations

Overview

Apprentices must complete 4 scenario demonstrations in which they will demonstrate the KSBs assigned to this assessment method. The scenarios will be simulated and provided remotely online by the EPAO.

The products of each scenario will be submitted to the assessor and these will be assessed. The scenario outputs will be supplemented by questioning.

The scenario demonstrations as well the questioning component must be completed within 10 days, starting from when the apprentice undertakes their first scenario demonstration.

The apprentice will be presented with scenarios relevant to their normal sphere of work, or sufficiently similar as to be equivalent in complexity, but which may use cyber challenges that are in a different business domain to the one in which they normally work.

The total time permitted for the scenario demonstrations is 7 hours 45 minutes typically over a minimum of 2 consecutive working days. A working day is typically considered to be 7.5 hours long.

The EPAO will agree the scheduling of the scenario demonstrations and questioning with the employer.

The rationale for this assessment method is:

Scenario demonstrations allow a demonstration of competence and involve direct testing under controlled conditions. Undertaking the scenario demonstrations in a controlled environment allows for pre-determined independent assessor training and assessment resources to be developed and helps to guarantee the required demand and challenges that appear during this end point assessment method.

In this occupation an observation of practice in a live setting was not selected, as the apprentice is not likely to cover the breadth and depth of practice required within a reasonable EPA period. Scenario demonstrations avoid situations where occupational activities are not available or do not occur on the day and avoids issues around confidentiality or exposing an organisation’s confidential information. The apprentice will be presented with scenarios where they will be able to demonstrate how they can apply their knowledge, skills and behaviours.

Delivery

One week in advance of the scenario demonstrations the EPAO must provide the apprentice and employer with a guidance document, with information on the format of the test, including timescales. No information on the context of the individual scenarios will be included within the guidance document.

On the day of the scenario demonstration apprentices must be provided with clear instructions on the tasks they must complete, including the timescales they are working to. The apprentice will be given access to the simulated environment, background material, and guidance provided by the EPAO that is appropriate to each of the 4 scenarios for the demonstrations on the day of the scenario-based demonstration. No additional clarification or guidance may be provided by the independent assessor, nor the invigilator, nor any other person. The scenario demonstrations should be conducted in the following way to take account of the occupational context in which the apprentice operates:

The scenario demonstrations will each take the allotted amount of time as specified below:

- Attack and Threat Research 1 hour 45 minutes
- Risk Assessment 2 hours
- Set up and configure a system with security features 3 hours
- Computer programme/script writing 1 hour

Each of the 4 scenario demonstrations may not be split, other than to allow comfort breaks as necessary. Once a scenario demonstration has been started it must be completed on the same day to ensure the security of the assessment.

The following activities MUST be demonstrated during the practical demonstration, that is, a practical demonstration without these tasks would seriously hamper the opportunity for the apprentice to demonstrate occupational competence in the KSBs assigned to this assessment method.

Scenario 1 Attack and Threat Research

The following activities must be covered during the practical demonstration:

- research current threat and attack techniques
- discover vulnerabilities in a provided computer system
- describe the significance of threat research and vulnerability discovery in a given context in an electronic document within the scenario

Scenario 2 – Risk Assessment

The following activities must be covered during the practical demonstration:

- conduct a risk assessment
- produce an electronic document that proposes mitigations with a supporting a rationale appropriate to the context of the employer within the scenario

Scenario 3 - Set up and configure a system with security features

The following activities must be covered during the practical demonstration:

- set up a system that incorporates a computer, a network, and a cyber-security function (components to be provided and may be virtual, design to be provided) and demonstrate that it functions as intended.

- configure all the main parts of the system (computer, network, and cyber security function) to implement the controls identified in a supplied security case.
- demonstrate that security controls are effective against the intended threat.

Scenario 4 Computer programme/script writing

The following activities must be covered during the practical demonstration:

- write a program or script to meet a given requirement
- demonstrate that the programme or script functions as intended and has been written to a coding standard that the apprentice is familiar with from their apprenticeship

A script may automate port scanning, or analyse data in a spreadsheet.

The script or programme should be of equivalent coding complexity. The scenario may offer a range of languages and scripts for a given problem i.e. the apprentice has a choice of which to use.

The 4 scenarios do not have to follow immediately after each other. The order in which the scenarios are undertaken is not prescribed. The scenario questioning period may not commence until all 4 scenario demonstrations have completed. The scenario-based demonstrations may be scheduled over several days if necessary.
The apprentice will be given one demonstration at a time and must complete that scenario demonstration before moving on to the next, based on the individual scenario timings provided.

The scenario demonstrations must be invigilated. The invigilation will be carried out by the independent assessor or a responsible person in accordance with EPAO guidelines. Invigilation can be carried out remotely or face to face. The EPAO is required to have an invigilation policy that will set out how the scenario demonstrations will be invigilated.

The EPAO is responsible for ensuring the security of scenario demonstrations they administer to ensure the assessment remains valid and reliable. This includes any arrangements for access to any data source locations which may be available locally or online.

If the scenario demonstration is conducted via live streaming, the EPAO must ensure that the apprentice is unable to gain an advantage through materials in the room, screen sharing or other behaviours.

No materials created during the assessment or copies of the scenario content are to be retained by the apprentice after the scenario demonstrations are complete.

EPAOs will create and set mark schemes to assess related underpinning KSBs within the scenarios.

KSBs demonstrated within the outputs of the scenario demonstrations must be documented by the independent assessor.

The independent assessor will make all grading decisions.

Questions and resources development

EPAOs will create and set scenario demonstrations to assess related underpinning KSBs.

EPAOs will produce specifications to outline in detail how the scenario demonstrations will operate and what they will cover. It is recommended that this be done in consultation with employers. EPAOs should put measures and procedures in place to maintain the security and confidentiality of their specifications if employers are consulted. Specifications must be standardised by the EPAO.

EPAOs must develop 'practical scenario banks' of sufficient size to prevent predictability and review them regularly (and at least once a year) to ensure they, and the specifications they contain, are fit for purpose. The scenario specifications, including questions relating to underpinning KSBs must be varied, yet allow assessment of the relevant KSBs.

Venue

The EPAO must verify the suitability of the venue for carrying out the demonstrations and the identity of the person taking the test. The EPAO may inspect the venue at their discretion. Apprentices must undertake the demonstrations in a suitably controlled environment that is a quiet space, free of distractions and influence.

Scenario demonstrations can be conducted in one of the following locations:

- the employer's premises
- a suitable venue selected by the EPAO (e.g. a training provider's premises or another employer's premises)
- online via live streaming

Support material

EPAOs will produce the following material to support this assessment method:

- independent assessor training materials
- grading guidance
- outline of the assessment method's requirements
- marking materials
- guidance document for employers and apprentices on the process/timescales for this assessment method as well as a description of the purpose
- guidance document for independent assessors on how to carry out the assessment

Component 2 – Questioning

Delivery

The scenario demonstrations will be supplemented by questioning following the independent assessors review of all 4 scenario demonstration outputs.

The independent assessor should have 5 days to review the scenario demonstration outputs and generate appropriate questions. The independent assessor is responsible for generating suitable questions in line with the EPAO's training and standardisation process.

The purpose of questioning is to help the assessor assess the apprentice's understanding of underpinning reasoning for their actions within the scenarios for the KSBs assigned to this method as evidenced in the scenario demonstration activity. Questioning should not be used to extend the scope of the assessment and should focus on the outputs of each scenario demonstration. Those KSBs that the apprentice did not have the opportunity to demonstrate during the scenario demonstration outputs can instead be covered by questioning, although these should be kept to a minimum.

Questioning must last 45 minutes and is in addition to the total time for the scenario demonstration (component 1). The independent assessor has the discretion to increase the duration of questioning by up to 10% to allow the apprentice the opportunity to respond to their final question. The time for questioning can be allocated across the scenarios according to the judgement of the assessor of where questions will add most value in increasing their understanding of the competence of the apprentice.

The independent assessor must use the full time available for questioning to allow the apprentice the opportunity to evidence occupational competence at the highest level available unless the apprentice has already achieved the highest grade available.

The independent assessor must ask a minimum of 9 questions typically focussed on scenarios 1 to 3 at their discretion. Follow up questions may be asked where clarification is required.

During the questioning component, apprentices must be provided with a copy of the outputs from their scenario demonstrations to refer to and to aid recall. This can be done via paper-based outputs of via a screen share facility.

The assessment must be documented by the independent assessor with a recording kept by the EPAO for quality assurance purposes. The independent assessor will assess all components of this assessment method holistically.

Questions and resources development

Independent assessors are responsible for generating suitable questions in line with the EPAO's training and standardisation process.

EPAOs must ensure that apprentices have a different set of questions in the case of re-sits/re-takes.

Independent assessors must be developed and trained by the EPAO in the conduct of questioning and reaching consistent judgement.

EPAOs will produce specifications to outline in detail how the questioning will operate, what it will cover and what should be looked for. It is recommended that this be done in consultation with employers. EPAOs should put measures and procedures in place to maintain the security and confidentiality of their questions if employers are consulted. EPAO must have a system in place to assure that the Questions are relevant, effective and fair, providing for consistency of assessment standards across different employers and apprentices.

Venue

Questioning must be conducted in one of the following locations:

- the employer's premises

- a suitable venue selected by the EPAO (e.g. a training provider's premises or another employer's premises)
- online via live streaming

Support material

EPAOs will produce the following material to support this assessment method:

- independent assessor training materials
- grading guidance
- outline of the assessment method's requirements
- marking materials
- guidance document for employers and apprentices on the process/timescales for this assessment method as well as a description of the purpose
- guidance document for independent assessors on how to carry out the assessment

Assessment method 3: Project Report (This assessment method has 1 component.)

Overview

Apprentices will conduct a project and submit a project report to the EPAO. The project is compiled after the apprentice has gone through the gateway.

The work-based project should be designed to ensure that the apprentice's work meets the needs of the business, is relevant to their role and allows the relevant KSBs to be demonstrated for the EPA. Therefore, the project's subject, title and scope will be agreed between the employer and the EPAO at the gateway. The employer will ensure it has a real business application and the EPAO will ensure it meets the requirements of the EPA (including suitable coverage of the KSBs assignment to this assessment method).

The rationale for this assessment method is:

Cyber Security Technologists work in a project-based environment and are responsible for carrying out cyber security activities and implementation of cyber security solutions. The project will address a cyber security engineering issue, a risk assessment issue, or a defend and respond issue, tailored to the cyber security specialism of the apprentice's employer which reflects the normal working practices within the role. As part of the role they will be expected to complete project reports and the project will reflect the areas their report would cover within the industry.

Each project will focus on the specialism undertaken by the apprentice within the Cyber Security Technologist standard and may be based on any of the following:

- a specific problem
- a recurring issue
- an idea/opportunity

Example project titles for each option within the occupational standard are listed below for illustrative purposes:

Cyber Security Engineer Option

- design and configure a network to meet a requirement and troubleshoot to optimise performance
- analyse requirements and build a security system to provide effective defence against cyber threats.

Risk Analyst Option

- undertake a cyber risk assessment and produce a report
- participate in a cyber-security audit and produce a report
- undertake a cyber-security culture assessment and design and implement a security awareness campaign
- undertake a security policy review and produce a report

Cyber Defender & Responder Option

- develop an incident response plan for approval within an organisations' governance arrangements for incident response.
- manage local response to non-major incidents in accordance with a defined procedure.
- detect and analyse a security incident with action plan responses.
- implement security tool configuration in response to threat intelligence

The above projects are suggestions, other appropriate projects are permitted.

Delivery

Apprentices will conduct a project and submit an electronic based project report. The format of the project report may vary in presentation style dependant on the option being taken.

The project is undertaken, and report compiled after the apprentice has gone through the gateway. The apprentice will conduct their project and submit a project report to the EPAO after a maximum of 6 weeks from the EPA start date.

The employer will ensure the apprentice has sufficient time and the necessary resources, within this period, to plan and undertake the project.

Whilst completing the project, the apprentice should be subject to normal workplace supervision. The apprentice may work as part of a team which could include technical internal or external support however the report will be the apprentice’s own work and will be reflective of their own role and contribution.

The apprentice will need to consider the availability of company and external resources required to complete their project. They must also ensure they are fully aware of the KSBs the project is intended to assess.

The project report has a **maximum** word limit of 2,000 words. A tolerance of plus or minus 10% is allowed. Appendices, references, diagrams etc will not be included in this total.

Where organisational documents are required, screenshots or extracts should be provided. Hyperlinks to external sources will not be permitted.

All project reports (irrespective of the option chosen) should include:

- an introductory section (text only, i.e. no diagrams, screen shots or figures) that explains:
  - description of the project
  - approach
  - project outcomes
  - how the KSB are evidenced through the project

For **Cyber Security Engineer Option,** the Project report must cover the following additional headings:

- design of the network
- evidence that the network works to meet the requirement
- network optimisation metrics against performance requirements
- requirements analysis and its link to the eventual system, including security features
- schematics to show the build of a system to the design from provided components
- configuration metrics to show how the system to meet the security requirements
- demonstration of how the security features are effective

For **Cyber Risk Analyst Option**, the Project Report must cover the following additional headings:

- description of the role taken in a cyber security risk assessment and audit
- a report explaining the conduct of the risk assessment & audit
- a report considering the cyber policies and cyber awareness campaign

For **Cyber Security Defender and Responder Option** the Project Report must cover the following additional headings:

- incident manager report of an incident response
- incident response plan submitted for approval
- detection of a security incident and action taken
- analysis of a security incident and action taken
- evidence of the implementation of tool configuration in response to threat intelligence

The project report must map, in an appendix, how it evidences the relevant KSBs for this assessment method.

When the project is submitted, the employer and the apprentice must verify that the submitted work is that of the apprentice.

Marking

The independent assessor will review and mark the project in a timely manner, as determined by the EPAO, and without extending the EPA unnecessarily. Similarly, all quality control processes will also be conducted in a timely manner, as determined by the EPAO.

Supporting material

EPAOs will produce the following material to support this assessment method:

- independent assessor training materials
- grading guidance
- outline of the assessment method's requirements
- marking materials
- guidance document for employers and apprentices on the process/timescales for this assessment method as well as a description of the purpose
- guidance document for independent assessors on how to carry out the assessment

Assessment method 4 – Knowledge Test (This assessment method has 1 component.)

Overview

A knowledge test is a controlled assessment which consists of a series of questions in which apprentices are asked to provide a response.

The rationale for this assessment method is:

This will allow the KSBs which may not naturally occur in every workplace or may take too long to observe to be assessed and the assessment of a disparate set of knowledge requirements. The test is mapped to knowledge statements that could not be fully assessed in the other three assessment methods.

Test Format

The knowledge test will consist of 40 multiple-choice questions. The multiple-choice questions will have four options of which one will be correct. The questions must be varied, to avoid the test becoming too predictable, yet allow assessment of the relevant KSBs.

The knowledge test can be:

- computer based
- paper-based

The questions must be split equally between the two knowledge statements.

Test administration

Apprentices must have a maximum of 60 minutes to complete the test.

The test is closed book which means that the apprentice cannot refer to reference books or materials.

Marking

Multiple-choice tests must be marked by independent assessors or markers employed by the EPAO following a marking guide produced by the EPAO. Alternatively, marking by computer is permissible where questions types allow this.

A correct response will be assigned one mark.

Any incorrect or missing answers must be assigned zero marks.

Assessment location

Apprentices must take the test in a suitably controlled environment that is a quiet space, free of distractions and influence, in the presence of an invigilator. The invigilator may be another external person employed by the EPAO or specialised (proctor) software if the test can be taken on-line. The EPAO is required to have an invigilation policy that will set out how the test/examination is to be carried out. This will include specifying the most appropriate ratio of apprentices to invigilators to best consider the setting and security required in administering the test/examination.

The EPAO is responsible for ensuring the security of testing they administer to ensure the test remains valid and reliable (this includes any arrangements made using online tools). The EPAO is responsible for verifying the validity of the identity of the person taking the test.

Question and resources development

Independent assessors are responsible for generating suitable questions in line with the EPAO's training and standardisation process. Questions must be relevant to the occupation and employer settings. It is recommended that this be done in consultation with employers of this occupation. EPAOs must have systems to maintain the security and confidentiality of questions asked by assessors. The system should ensure questions are not predictable and the quality of them is assured to be fit for purpose.

Required supporting material

As a minimum EPAOs will produce the following material to support this method:

- a question bank
- a multiple-choice test specification
- sample multiple-choice tests and mark schemes
- live multiple choice tests and mark schemes
- analysis reports which show areas of weakness for completed multiple-choice tests/exams and an invigilation policy

Reasonable adjustments

The EPAO must have in place clear and fair arrangements for making reasonable adjustments for this apprenticeship standard. This should include how an apprentice qualifies for reasonable adjustment and what reasonable adjustments will be made. The adjustments must maintain the validity, reliability and integrity of the assessment methods outlined in this assessment plan.

Weighting of assessment methods

All assessment methods are weighted equally in their contribution to the overall EPA grade.

Grading

Assessment method 1: Professional discussion underpinned by portfolio

A fail is where the evidence does not meet all the pass criteria

Core		
KSBs	**Pass** **Apprentices must meet all the pass descriptors**	**Distinction** **Apprentices must meet all the pass descriptors plus all of the distinction descriptors.**
K3 K6 K7 K8 K9 K15 S6 S7 S9 S15 B3 B4 B5 B6 B7 B8	Identifies and describes cyber security concepts (including the meaning of terms in a cyber security context and how they relate to each other: identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard) and assesses their relevance to business and society, explaining how achieving security outcomes leads to benefits in practice. K3 Explains security assurance concepts including reference to what assurance is for in security, and 'trustworthy' versus 'trusted' and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods. K3 Explains life cycle and service management practices with reference to an established standard at foundation level. K6 Explains how they advised others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation. K7	Critically evaluates the impact of cyber security concepts on an organisation explaining how they bring benefits by exploring the interrelation of risk and harm. K3 Critically analyses different views of the future and trends in threat, and after assessing the implications for the organisation/business, recommends changes that reduce risk with justification. S9 Evaluate their use of tools and techniques, justifying their selection to prevent a breach to digital system security. S15

	Explains the main features, applicability and how to apply the significant law, regulations and standards relevant specifically to cyber security. K8 Discusses the ethical principles and codes good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional. K9 Summarises how a security management system works, including how governance, organisational structure, roles, policies, standards, guidelines combine effectively to achieve the intended security outcomes. K15 Explains how they have analysed simple security cases without supervision including the security objectives, threats, and for every identified attack technique identify mitigation or security controls that could include technical, implementation, policy, or process. S6 Identifies their organisational policies and standards for information and cyber security and able to operate according to service level agreements or other defined performance targets and describes how they ensure that they follow them. S7 Explains how they have reviewed the employers cyber security posture and made recommendations for improvement having investigated different views of the future and trends in technology and threats (using more than 1 external source) reflecting on what the implications are for the organisation/business. S9 Explains how to use tools, techniques and processes to prevent a breach to digital system security. S15 Describes how they establish an independent approach to work tasks which reflect the	

	instructions/policies/guidelines/procedures set out by the organization. B3 Describes how they have shown initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit. B4 Explains how they respond to work tasks with an organized approach which reflects the time limits/guidelines set out by their employer. B5 Explains how they establish relationships with co-workers and stakeholders which follows the inclusion and diversity policies of the organisation. B6 Explains how they establish a style of communication which reflects the audience and situational context and adapts this style to present the same information to technical and non-technical audiences. B7 Describes their approach to productivity, professionalism and the security of the working environment which reflects standard operating procedures and the principles/policies/guidelines set out by the organization. B8	

Assessment method 2: Scenario Based Demonstration

A fail is where the evidence does not meet all the pass criteria

KSBs	Pass Apprentices must meet all the pass descriptors	Distinction Apprentices must meet all the pass descriptors plus all of the distinction descriptors.
Scenario 1 Attack and Threat Research K4 K5 K11	Identifies the common attack techniques and explains ways to defend or mitigate them. K4	Critically evaluates how threats have been identified and their impact/relevance to a system and organization. S1 S17

S1 S2 S3 S17 B2 B9 B10	Explains the role of human behaviour in cyber security risk, including the significance of the ‘insider threat’. K4 Explains how attack techniques combine with motive and opportunity to become a threat. K4 Identifies the significance of trends in cyber security threats and includes in their cyber security strategy an understanding of and the value and risk of this analysis showing how they deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment. K5 Outlines the procedure for accessing and applying sources of threat intelligence and vulnerabilities for horizon scanning. K11 Performs research and exploration) to identify vulnerabilities in a system. S1 Analyses and evaluates security threats and hazards to a system or service or processes using relevant external source of threat intelligence or advice (e.g. National Cyber Security Centre) to create an enriched view from a combination of different sources. S2 Researches and investigates common attack techniques and relates these to normal and observed digital system behaviour. S3 Interprets and demonstrates use of at least one external source of vulnerabilities (e.g. OWASP, intelligence sharing initiatives, open source). S3	

	Identifies threats relevant to a specific organisation and/or sector within the scenario. S17 Establishes and analytical approach - working with data effectively to see patterns, trends and draw meaningful conclusions. B2 Establishes a creative approach to cyber security by taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, and bringing novel and unexpected solutions to address cyber security challenges. B9 Responds to problems with an approach that reflects how they have identified cyber issues quickly ensuring the true root cause of any problem is found and applied appropriate solutions which prevent recurrence. B10	
Scenario 2 Risk Assessment K14 S4 S27 B1	Identifies and applies cyber security risk assessment and audit methodologies and approaches to risk treatment in the context of a system or organisation. K14 Identifies vulnerabilities in an organisation and its security management system. K14 Explains the threat intelligence lifecycle. Describes different approaches to risk treatment and contrasts the role of the risk owner with other stakeholders. K14 Undertakes a security risk assessment for a simple system without direct supervision and proposes basic remediation advice in the context of the scenario employer. S4	Evaluates employer relevance of risk assessment outcomes i.e. why is a proposal beneficial to relevant stakeholders. K14 S4 Optimise outcomes by choosing counter measures to minimise business impact. K14 S4

	Demonstrates the recording and reporting of appropriate information, including written reports within a structure or template provided. S27 Demonstrates logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions. B1	
Scenario 3 Set up and Configure a security System K2 K10 K12 K16 S5 S8	Explains the use of at least three Operating System (OS) security functions and associated features to resolve a cyber issue. K2 Implements a requirements analysis and develops a security case including context, threats, how to derive security objectives justifying the selected mitigations and security controls with reasoning and recognising the dynamic and adaptable nature of threats, in a representative business scenario. K10 Evaluates common security architectures and methodologies and demonstrates how cyber security technology components are typically deployed in digital systems to provide security functionality including: hardware and software to implement security controls. K12 Demonstrates an understanding of the function and features of significant digital system components; typical architectures; common vulnerabilities in digital systems. K16 Undertakes activities using the principles and common practice present in digital system security. K16 Analyses a security case and describes what threats, vulnerability	Evaluates the significance of the selected security controls within the exercise providing explanation for their choice. K10 Evaluates the consequences and trade-offs of the selection of security components within the exercise. K12 Explains the rationale and consequences for the threats vulnerabilities and risks selected versus those discarded. S5

	or risks are mitigated and identifies any residual areas of concern. S5 Configures, deploys, and uses computer, digital network and cyber security technology. S8	
Scenario 4 Computer Programme/Script writing K17 S13	Writes program code or scripts to meet a given design requirement in accordance with employers' coding standards. K17 S13	

Assessment method 3: Project report

A fail is where the evidence does not meet all the pass criteria

Option 1- Cyber Security Engineer		
KSBs	**Pass** **Apprentices must meet all the pass descriptors**	**Distinction** **Apprentices must meet all the pass descriptors plus all of the distinction descriptors.**
S10 S11 S12 S14	Designs, builds tests and troubleshoots a network incorporating more than one subnet with static and dynamic routes, that includes servers, hubs, switches, routers, and user devices to a given design requirement without supervision. S10 Analyses functional and non-functional security requirements presented in a security case against other design requirements identifying conflicts and justifying a solution based on valid trade-offs. S11 Designs and builds, within broad but generally well-defined parameters, a system in accordance with a security case, including selection and configuration of typical security hardware and software components	Evaluates network performance with reference to the design requirements and identifies using troubleshooting techniques ways to implement improvements. S10 Analyse the rationale and consequences of the selection of typical security components for the business. S12 Critically evaluate the use of encryption and the plan for the management of encryption keys in terms of the usability, costs and benefits for relevant stakeholders. S14

	for example a system at the enterprise, network or application layer ensuring that the system has properly implemented security controls as required by the security case. S12 Designs a system employing encryption to meet defined security objectives and develops and implements a plan for managing the associated encryption keys for the given system. S14	

Option 2- Cyber risk assessor		
KSBs	**Pass**	**Distinction**
S16 S18 S19 S20 S22 S23 S24	Conducts a cyber-risk assessment against an externally (market) recognised cyber security standard using a recognised risk assessment methodology. S16 Develops an information security policy or process to address identified risks for example from security audit recommendations. S18 Develops an information security policy within a defined scope to take account of relevant cyber security legislation and regulation. S19 Implements part of a security audit against a recognised cyber security standard, undertake a gap analysis and makes recommendations for remediation. S20 Develops a local business continuity plan for approval within an organisations' governance arrangements for business continuity. S22	Analyses the rationale and consequences of the design of a typical information security policy for the business S19 Analyses the rationale and consequences of the design of a typical business continuity plan for the business S22 Evaluates with evidence the outcomes from a security awareness campaign and propose improvements S24

	Assesses security culture using a recognised approach. S23 Designs and implements a simple 'security awareness' campaign to address a specific aspect of a security culture. S24	

Option 3- Cyber defend and respond		
KSBs	**Pass**	**Distinction**
S21 S25 S26 S28 S29 S30	Develops an incident response plan for approval within an organisations' governance arrangements for incident response. S21 Integrates and correlates information from various sources (including log files from different sources, digital system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compares organisational data to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a digital system security breach. S25 Recognises anomalies in observed digital system data structures (including by inspection of network packet data structures) and digital system behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools. S26 Configures digital system monitoring and analysis tools (e.g. SIEM tools), taking account of	Analyses the rationale and consequences of the design of a typical incident response plan for the employer, business, or organization. S21 Evaluates how the recognised incidents demonstrate the threat actors' approach i.e. what is going on that causes the observed anomalies and what the motive could be. S25 S26 Analyses the rationale and consequences of selecting and configuring digital system monitoring tools for the employer, business, or organization. S28

	threat & vulnerability intelligence, indicators of compromise. S28 Undertakes root cause analysis of events and makes recommendations to reduce false positives and false negatives. S29 Manages local response to non-major incidents in accordance with a defined procedure. S30	

Assessment method 4: Knowledge Test

The following grade boundaries apply to the test:

Grade	Minimum score	Maximum score
Pass	25	40
Fail	0	24

The questions within the test must be divided between the Knowledge Statements to be tested such that K1 and K13 each have 20 questions.

Overall EPA grading

All EPA methods must be passed for the EPA to be passed overall.

Grades from individual assessment methods should be combined in the following way to determine the grade of the EPA as a whole:

Assessment method 1 – Professional discussion	Assessment method 2 – Scenario based demonstration	Assessment method 3 – Project report	Assessment Method 4 – Knowledge test	Overall grading
Fail	Any grade	Any grade	Any grade	Fail
Any grade	Fail	Any grade	Any grade	Fail
Any grade	Any grade	Any grade	Fail	Fail
Any grade	Any grade	Fail	Any grade	Fail
Pass	Pass	Pass	Pass	Pass
Distinction	Pass	Pass	Pass	Pass
Pass	Distinction	Pass	Pass	Pass
Pass	Pass	Distinction	Pass	Pass

Distinction	Distinction	Pass	Pass	Merit
Distinction	Pass	Distinction	Pass	Merit
Pass	Distinction	Distinction	Pass	Merit
Distinction	Distinction	Distinction	Pass	Distinction

Re-sits and re-takes

Apprentices who fail one or more assessment method will be offered the opportunity to take a re-sit or a re-take at the employer's discretion. The apprentice's employer will need to agree that either a re-sit or re-take is an appropriate course of action.

A re-sit does not require further learning, whereas a re-take does.

Apprentices should have a supportive action plan to prepare for a re-sit or a re-take.

An apprentice who fails one or more assessment method, and therefore the EPA in the first instance, will be required to re-sit or re-take the failed assessment method(s) only.

The timescales for a re-sit/re-take is agreed between the employer and EPAO. A re-sit is typically taken within two 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 four months of the EPA outcome notification.

All assessment methods must be taken within a six-month period, otherwise the entire EPA will need to be re-sat/re-taken.

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

Where any assessment method must be re-sat or re-taken, the apprentice can still achieve a distinction grade overall.

Roles and responsibilities

Role	Responsibility
Apprentice	As a minimum, apprentices should: • participate in and complete on-programme training to meet the KSBs as outlined in the occupational standard for a minimum of 12 months • undertake 20% off-the-job training as arranged by the employer and training provider • understand the purpose and importance of EPA • undertake the EPA including meeting all gateway requirements
Employer	As a minimum, employers should: • work with the training provider (where applicable) to support the apprentice in the workplace to provide the opportunities for the apprentice to develop the KSBs • arrange and support a minimum of 20% off-the-job training to be undertaken by the apprentice • decide when the apprentice is working at or above the occupational standard and so is ready for EPA • select the EPAO • ensure that all supporting evidence required at the gateway is submitted in accordance with this EPA plan • remain independent from the delivery of the EPA • confirm arrangements with the EPAO for the EPA (who, when, where) in a timely manner (including providing access to any employer specific documentations as required, for example company policies) • ensure that the EPA is scheduled with the EPAO for a date and time which allow appropriate opportunity for the KSBs to be met • ensure the apprentice is well prepared for the EPA • ensure the apprentice is given sufficient time away from regular duties to prepare for and complete all post-gateway elements of the EPA, and that any required supervision during this time (as stated within this EPA plan) is in place

	• where the apprentice is assessed in the workplace, ensure that the apprentice has access to the resources used on a daily basis
EPAO	As a minimum, EPAOs should: • agree the EPA price • understand the occupational standard • appoint administrators (and invigilators where required) to administer the EPA as appropriate • provide training for independent assessors in terms of good assessment practice, operating the assessment tools and grading • provide adequate information, advice and guidance documentation to enable apprentices, employers and training providers to prepare for the EPA • arrange for the EPA to take place, in consultation with the employer • deliver the EPA as outlined in this EPA plan in a timely manner use appropriate assessment recording documentation to ensure a clear and auditable process is in place for providing assessment decisions and feedback to all relevant stakeholders • have no direct connection with the apprentice, their employer or training provider. In all instances including when the EPAO is the training provider (i.e. HEI) there must be no conflict of interest • have policies and procedures for internal quality assurance (IQA), and maintain records of regular and robust IQA activity and moderation for external quality assurance (EQA) purposes • conform to the requirements of the nominated external quality assurance provider (EQAP) • conform to the requirements of the Register of End-Point Assessment Organisations (RoEPAO) • deliver induction training for independent assessors, and for invigilators and markers where used • undertake standardisation activity on this apprenticeship standard for all independent assessors before they conduct an EPA for the first time, if the EPA is updated and periodically as appropriate (a minimum of annually)

	• manage invigilation of apprentices to maintain security of the assessment in line with their malpractice policy • verify the identity of the apprentice being assessed • use language in the development and delivery of the EPA that is appropriate to the level of the occupational standard • request certification via the Apprenticeship Service upon successful achievement of the EPA • develop and produce assessment materials including specifications and marking materials (for example mark schemes, practice materials, training material) • appoint suitably qualified and competent independent assessors • provide details of the independent assessor's name and contact details to the employer • have and apply appropriately an EPA appeals process
Independent assessor	As a minimum, an independent assessor should: • have the competence to assess the apprentice at this level and hold any required qualifications and experience in line with the requirements of the independent assessor as detailed in the IQA section of this EPA plan • understand the occupational standard and the requirements of this EPA • have, maintain and be able to evidence up to date knowledge and expertise of the subject matter • deliver the end-point assessment in-line with the EPA plan • comply with the IQA requirements of the EPAO • have no direct connection or conflict of interest with the apprentice, their employer or training provider; in all instances including when the EPAO is the training provider (i.e. HEI) • attend induction training • attend standardisation events when they begin working for the EPAO, before they conduct an EPA for the first time and a minimum of annually on this apprenticeship standard • assess each assessment method, as determined by the EPA plan, and without extending the EPA unnecessarily

	• assess against the KSBs assigned to each assessment method, as shown in the mapping of assessment methods, and as determined by the EPAO, and without extending the EPA unnecessarily • make all grading decisions • record and report all assessment outcome decisions, for each apprentice, following instructions and using assessment recording documentation provided by the EPAO, in a timely manner • use language in the development and delivery of the EPA that is appropriate to the level of the occupational standard
Training provider	As a minimum, the training provider should: • work with the employer and support the apprentice during the off-the-job training to provide the opportunities to develop the knowledge, skills and behaviours as listed in the occupational standard • conduct training covering any knowledge, skill or behaviour requirement agreed as part of the Commitment Statement (often known as the Individual Learning Plan). • monitor the apprentice's progress during any training provider led on-programme learning • advise the employer, upon request, on the apprentice's readiness for EPA • remain independent from delivery of the EPA. Where the training provider is the EPA (i.e. a HEI) there must be procedures in place to mitigate against any conflict of interest
Marker	As a minimum, the marker should: • attend induction training • have no direct connection or conflict of interest with the apprentice, their employer or training provider in all instances including when the EPAO is the training provider (i.e. HEI) • mark multiple-choice test answers accurately according to the EPAO's mark scheme and procedures
Invigilators	As a minimum, invigilators should: • attend induction training as directed by the EPAO

	• have no direct connection or conflict of interest with the apprentice, their employer or training provider; in all instances, including when the EPAO is the training provider (i.e. HEI) • invigilate and supervise apprentices during tests and in breaks during assessment methods to prevent malpractice in accordance with the EPAO's invigilation procedures

Internal Quality Assurance (IQA)

Internal quality assurance refers to the strategies, policies and procedures that EPA organisations must have in place to ensure valid, consistent and reliable end-point assessment decisions. EPAOs for this EPA must adhere to all requirements within the Roles and Responsibilities section and:

- have effective and rigorous quality assurance systems and procedures that ensure fair, reliable and consistent assessment across employers, places, times and independent assessors
- appoint independent assessors who have recent relevant experience of the occupation/sector gained in the last three years or significant experience of the occupation/sector and evidence of continued professional development
- appoint independent assessors who are competent to deliver the end-point assessment and who meet the following minimum requirements:
    - experience of cyber security technology
    - evidence of continued professional development
- operate induction training for independent assessors, markers and invigilators
- provide training for independent assessors in terms of good assessment practice, operating the assessment tools and grading
- where appropriate:
    - provide ongoing training for markers
    - provide ongoing training for invigilators
- undertake standardisation activity on this apprenticeship standard for all independent assessors:
    - before they conduct an EPA for the first time
    - if the EPA is updated
    - periodically as appropriate (a minimum of annually)
- conduct effective moderation of assessment decisions and grades
- conduct appeals where required, according to the EPAO's appeals procedure, reviewing and making final decisions on assessment decisions and grades

Affordability

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

- using an employer's venue for applicable assessment methods
- using video conferencing or live streaming for applicable assessment methods
- the possibility of scheduling more than one assessment method on the same day

Professional body recognition

n/a for this occupation

Mapping of knowledge, skills and behaviours (KSBs)

Assessment method 1: Professional discussion underpinned by portfolio

Core Knowledge
K3 Cyber security concepts and why cyber security matters to business and society; Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods.
K6 Lifecycle and service management practices to an established standard to a foundation level for example Information Technology Infrastructure Library (ITIL) foundation level.
K7 Cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.
K8 Understands the main features, applicability and how to apply the significant law, regulations and standards relevant specifically to cyber security. To include: laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation); use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions..
K9 Ethical principles and codes for good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional.
K15 Principles of security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes.
Core Skills
S6 Analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification.
S7 Identify and follow organisational policies and standards for information and cyber security and operate according to service level agreements or other defined performance targets.
S9 Recommend improvements to the cyber security posture of an employer or customer based on research into future potential cyber threats and considering threat trends.
S15 Use tools, techniques, and processes to actively prevent a breach to digital system security.

Core Behaviours
B3 Works independently and takes responsibility. For example, works diligently regardless of how much they are being supervised, and stays motivated and committed when facing challenges.
B4 Show initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit.
B5 Thorough & organised. For example, uses their time effectively to complete work to schedule and takes responsibility for managing their own workload and time.
B6 Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion & diversity policy.
B7 Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences.
B8 Maintains a productive, professional, and secure working environment.

Assessment method 2: Scenario Based Demonstration with questioning

Core Knowledge
K2 the concepts, main functions and features of at least three Operating Systems (OS) and their security functions and associated security features.
K4 the main types of common attack techniques; also, the role of human behaviour, including the significance of the 'insider threat'. Including: - how attack techniques combine with motive and opportunity to become a threat. - techniques and strategies to defend against attack techniques and mitigate hazards.
K5 the significance of identified trends in cyber security threats and understand the value and risk of this analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment.
K10 how to analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification.
K11 horizon scanning including use of recognised sources of threat intelligence and vulnerabilities.
K12 common security architectures and methodologies; be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance. How cyber security technology components are typically deployed in digital systems to provide security functionality including: hardware and software to implement security controls.
K14 risk assessment and audit methodologies and approaches to risk treatment; approaches to identifying the vulnerabilities in organisations and security management systems; the threat intelligence lifecycle; the role of the risk owner in contrast with other stakeholders.
K16 function and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security.
K17 programming or scripting languages.

Core Skills
S1 Discover vulnerabilities in a system by using a mix of research and practical exploration.
S2 Analyse and evaluate security threats and hazards to a system or service or processes. Use relevant external source of threat intelligence or advice (e.g. National Cyber Security Centre) Combine different sources to create an enriched view of cyber threats and hazards.
S3 Research and investigate common attack techniques and relate these to normal and observed digital system behaviour and recommend how to defend against them. Interpret and demonstrate use of external source of vulnerabilities (e.g. OWASP, intelligence sharing initiatives, open source).
S4 Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.
S5 Source and analyse a security case and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern.
S8 Configure, deploy and use computer, digital network and cyber security technology.
S13 Write program code or scripts to meet a given design requirement in accordance with employers' coding standards.
S17 Identify threats relevant to a defined context.
S27 Accurately, objectively and concisely record and report the appropriate cyber security information, including in written reports within a structure or template provided.
Core Behaviours
B1 Logical - Applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions.
B2 Analytical - working with data effectively to see patterns, trends and draw meaningful conclusions.
B9 Creative - taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, bring novel and unexpected solutions to address cyber security challenges.
B10 Problem Solving - Identifies issues quickly, enjoys solving complex problems and applies appropriate solutions. Dedicated to finding the true root cause of any problem and find solutions that prevent recurrence.

Assessment method 3: Project based

Option 1 Cyber Engineer - Skills
S10 Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, to a given design requirement without supervision. Provide evidence that the system meets the design requirement.
S11 Analyse security requirements (functional and non-functional security requirements that may be presented in a security case) against other design requirements (e.g. usability, cost, size, weight, power, heat, supportability etc.), given for a given system or product. Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.

S12 Design and build, systems in accordance with a security case within broad but generally well-defined parameters. This should include selection and configuration of typical security hardware and software components. Provide evidence that the system has properly implemented the security controls required by the security case.
S14 Design systems employing encryption to meet defined security objectives. Develop and implement a plan for managing the associated encryption keys for the given scenario or system.
Option 2 Cyber Risk Assessor Skills
S16 Conduct a cyber-risk assessment against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.
S18 Develop information security policies or processes to address a set of identified risks, for example from security audit recommendations.
S19 Develop information security policies within a defined scope to take account of legislation and regulation relevant to cyber security.
S20 Take an active part in a security audits against recognised cyber security standards, undertake gap analysis and make recommendations for remediation.
S22 Develop plans for local business continuity for approval within defined governance arrangements for business continuity.
S23 Assess security culture using a recognised approach.
S24 Design and implement a simple ‘security awareness’ campaign to address a specific aspect of a security culture.
Option 3 Cyber Defend and Respond Skills
S21. Develop plans for incident response for approval within defined governance arrangements for incident response.
S25 Integrate and correlate information from various sources (including log files from different sources, digital system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a digital system security breach
S26 Recognise anomalies in observed digital system data structures (including by inspection of network packet data structures) and digital system behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools.
S28 Configure digital system monitoring and analysis tools (e.g. SIEM tools), taking account of threat & vulnerability intelligence, indicators of compromise.
S29 Undertake root cause analysis of events and make recommendations to reduce false positives and false negatives.
S30 Manage local response to non-major incidents in accordance with a defined procedure.

Assessment method 4: Knowledge Test

Core Knowledge
K1 Principles of networks: OSI and TCP/IP models, data, protocols and how they relate to each other; the main routing protocols; the main factors affecting network performance including typical failure modes in protocols and approaches to error control; virtual networking.

K13 The basic terminology and concepts of cryptography; common cryptography techniques in use; the importance of effective cryptography key management and the main techniques used; legal, regulatory and export issues specific to use of cryptography.