Institute for Apprenticeships & Technical Education

End-point assessment plan for Cyber Security Technician apprenticeship standard

Apprenticeship standard reference number	Apprenticeship standard level	Integrated end-point assessment
ST0865	3	No

Contents

Introduction and overview

This document sets out the requirements for end-point assessment (EPA) for the Cyber Security Technician 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 Technician apprentices, their employers and training providers.

Full time apprentices will typically spend 18 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 3 months, after the EPA gateway.

The EPA consists of 3 discrete assessment methods.

The individual assessment methods will have the following grades:

Assessment method 1: Scenario Demonstrations with questioning

- Fail
- Pass

Assessment method 2: Professional Discussion underpinned by Portfolio

- Fail
- Pass
- Distinction

Assessment method 3: Knowledge Test

- Fail
- Pass

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

- Pass
- Fail
- Distinction

EPA summary table

On-programme (typically 18 months)	Training to develop the occupation standard's knowledge, skills and behaviours (KSBs).
End-point assessment gateway	• Employer is satisfied the apprentice is consistently working at, or above, the level of the occupational standard. • English and mathematics Level 2 Apprentices must complete: • Portfolio of evidence
End-point assessment (which will typically take 3 months)	Assessment method 1: Scenario Demonstrations with questioning With the following grades: • Fail • Pass Assessment method 2: Professional Discussion underpinned by Portfolio With the following grades: • Fail • Pass • Distinction Assessment method 3: Knowledge Test With the following grades: • Fail • Pass
Professional recognition	Aligns with recognition by: • BCS,The Chartered Institute for IT - Associate BCS membership (AMBCS) and Professional • Registration for IT Technicians (RITTech) • Chartered Institute for Information Security – Accredited Affiliate

Length of end-point assessment period

The EPA will be completed within an EPA period lasting typically of 3 months, after the EPA gateway.

Order of assessment methods

The assessment methods can be delivered in any order.

Gateway

The EPA period should only start once the employer is satisfied that the apprentice is consistently working at or above the level set out in the occupational standard, that is to say they are deemed to have achieved occupational competence. 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.

For Scenario Demonstrations with Questioning:

- no specific requirements

For 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 must contain evidence related to the KSBs that will be assessed by the professional discussion
- the portfolio of evidence will typically contain 8 discrete pieces of evidence
    - the evidence should be presented in the following sections, each section typically including two pieces of evidence:
        - Section 1 Application of Information Security Policies and Procedures
        - Section 2 Cyber security awareness and culture
        - Section 3 Maintaining professional knowledge of cyber security developments
        - Section 4 Information security governance practice.
- 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/records, for example workplace policies/procedures, records
    - witness statements
    - annotated photographs
    - video clips (maximum total duration 5 minutes); the apprentice must be in view and identifiable at all times
    - This is not a definitive list; other evidence sources are allowed.
- The portfolio should not include any methods of self-assessment or self-reflection
- any employer contributions should focus on direct observation of performance (for example witness statements) rather than opinions
- the evidence provided must 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 is not directly assessed. It underpins the professional discussion and therefore should not be marked by the EPAO. EPAOs should review the portfolio in preparation for the professional discussion but are not required to provide feedback on the portfolio itself.
- The portfolio of evidence can be electronic or paper-based (or a mixture of both).

For Knowledge Test:

- no specific requirements

Assessment methods

Assessment method 1: Scenario Demonstrations with questioning (This assessment method has 1 component)

Overview

Apprentices must be observed by an independent assessor completing 4 practical scenario demonstrations, in a simulated environment, which will be made up of tasks that would naturally occur as a Cyber Security Technician. This will be supplemented by questioning by the independent assessor to establish the apprentice's understanding of underpinning reasoning. This approach will demonstrate the KSBs assigned to this assessment method. The end-point assessment organisation will arrange for the demonstrations to take place, in consultation with the employer. Scenario demonstrations must be carried out over a total assessment time of 5 hours +10% at the discretion of the independent assessor. The apprentice will be given one demonstration at a time by the independent assessor and they will complete each scenario demonstration and questioning before going on to the next demonstration.

The independent assessor may conduct and observe only one apprentice at a time during this assessment method.

The rationale for this assessment method is that:

Scenario demonstrations allow a demonstration of competence and involves 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. Scenario demonstrations avoids 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 an Information Pack, with information on the format of the test, including timescales as well as procedure and policy documents required as context for the scenarios. Apprentices can make notes on these documents and bring them to the scenario demonstration.

The scenario demonstrations should be conducted in the following way:

The apprentice will be presented with scenarios relevant to their normal sphere of work.

The scenario demonstrations with questioning will take a total of 5 hours.

The apprentice will be given 4 scenarios for the demonstrations, previously unseen, developed and provided by the EPAO. The scenarios can describe separate events or tasks or relate to one incident.

Each Scenario Demonstration will last 75 minutes (+10% at the discretion of the independent assessor). The apprentice will be provided with a scenario of no more than 250 words together with an Information Pack with supporting information (for example Screenshots, Data for analysis, Reports, Articles, Documentation).

The independent assessor can ask up to 5 questions during and after each scenario demonstration. All questions must be asked during the 75 minutes permitted for each scenario to allow the apprentice to evidence any gaps in KSBs not evidenced by the demonstration. Questions can be taken from an EPAO question bank or be those generated by the independent assessor. KSBs observed and answers to questions must be documented by the independent assessor.

The following activities MUST be observed during the practical demonstration as without these tasks it would seriously hamper the opportunity for the apprentice to demonstrate occupational competence in the KSBs assigned to this assessment method:

- Perform a cyber security operational task
- Implement a cyber security control where cryptography is required
- Modify a cyber security access control
- Scope a cyber security vulnerability assessment
- Evaluate the results of a cyber security vulnerability assessment
- Monitor, identify and describe an information security event
- Respond to and report upon an information security event
- Conduct an information security risk assessment
- The business impact and mitigation(s) for the management of risk
- Maintain a digital information asset inventory

Apprentices must conduct the demonstrations in a suitably controlled environment that is a quiet space, free of distractions and influence. The invigilation will be carried out by the independent assessor. The EPAO is required to have an invigilation policy that will set out how the scenario demonstrations will be carried out. 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 made using online tools). The EPAO is responsible for verifying the validity of the identity of the person carrying out the demonstrations.

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

There may be breaks during the practical demonstrations to allow the apprentice to move from one location to another and for meal breaks.

The independent assessor will make all grading decisions.

Scenarios

Scenarios will be based on the following 4 topics:

Scenario Demonstration 1 – Implementing Cyber Security Controls
Example content:

- Perform a cyber security operational task e.g. applying a security patch
- Apply a cyber security control where cryptography is required
- Demonstrate how to modify a cyber security access control in order to fulfil a change request

Scenario Demonstration 2 – Vulnerability Management
Example Content:

- Produce a document that describes the scope for a cyber security vulnerability assessment to be conducted
- Read a document containing the results of a cyber security vulnerability assessment, identify the risks and provide mitigations for each risk

Scenario Demonstration 3 – Incident Management
Example Content:

- Demonstrate how to monitor for the occurrence of a cyber security event
- Demonstrate how to identify and respond to a cyber security event of interest
- For a provided cyber security event of interest that has been observed, produce a brief document that:
    - Describes the cyber security event observed
    - The details of how the event was identified
    - What the response to the event was
    - Why the particular response was chosen

Scenario Demonstration 4 – Risk Management
Example Content:

- For a provided scenario, produce a document that details:
    - The cyber security risks present
    - The business impact of each risk identified
    - The mitigation(s) for the management of the identified risk(s)
- Demonstrate how to add or delete an asset from a digital information asset inventory

Questions and resources development

EPAOs will create and set open questions to assess related underpinning KSBs.

EPAOs will produce specifications to outline in detail how the practical demonstrations will operate, what they 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 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 scenarios they contain, are fit for purpose. The scenarios, including questions relating to underpinning KSBs must be varied, yet allow assessment of the relevant KSBs.

Venue

Scenario demonstrations 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)
- via video conference

The venue must:

- Have access to the Internet
- Be a controlled environment for the scenario demonstrations to be conducted.

Support material

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

- Outline of the assessment method's requirements
- Marking materials
- Reference policies and procedures for the scenario demonstrations
- A question bank of open questions to assess related underpinning knowledge, skills and behaviours
- A guidance document, with information on the format of the test, including timescales
- Provide the grading criteria for the independent assessors to use and record

Assessment method 2: 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 excellence and cover the KSBs assigned to this assessment method. It will involve questions that will focus on coverage of prior learning or problem solving.

The rationale for this assessment method is that a professional discussion allows a two-way dialogue between the apprentice and independent assessor. It allows the apprentice to evidence how they have met the KSBs which are underpinned by evidence drawn from their portfolio. A professional discussion is a well-recognised method and 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.

Delivery

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

The professional discussion must last for 60 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 must combine questions from the EPAO's question bank and those generated by themselves. The independent assessor will ask a minimum of 10 questions.

The professional discussion is a structured one-to-one discussion between the apprentice and an independent assessor and must be appropriately structured to draw out the best of the apprentice's competence and excellence.

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 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 can draw on the contents of the portfolio to underpin the discussion, selecting items to inform and enhance their answers.

Video conferencing can be used to conduct the professional discussion, but the EPAO must have processes in place to verify the identity of the apprentice and ensure the apprentice is not being aided in some way.

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

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)
- via video conference

Other relevant information

A structured test specification and question bank must be developed by EPAOs. The 'question bank' must be of sufficient size to prevent predictability and the EPAO must reviewed regularly (at least once a year) to ensure that it, and its content, are fit for purpose. The specifications, including 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 discussion and reaching consistent judgement.

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

- Outline of the assessment method's requirements

- A structured discussion point template for the independent assessor to use and record on during the professional discussion
- The discussion areas mapped to KSBs
- A grading matrix for the independent assessor to use
- A bank of questions that address all KSBs mapped to this assessment method

Assessment method 3: Knowledge Test (This assessment method has 1 component)

Overview
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 two assessment methods.

Test Format
The test can be computer based and consist of 40 closed response questions (e.g. multiple-choice questions).

Test administration
This assessment method will be carried out as follows:

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.

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 take into account 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.

The test will be conducted in a suitably controlled environment that is a quiet space, free of distractions and influence, in the presence of an invigilator.

The EPAO must verify the suitability of the venue for taking the test and the identity of the person taking the test.

Marking
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.

Question and resources development

Questions must be written by EPAOs and must be relevant to the occupation and employer settings. It is recommended that this be done in consultation with employers of this occupation. EPAOs should also maintain the security and confidentiality of their questions when consulting employers. EPAOs must develop 'question banks' of sufficient size to prevent predictability and review them regularly (and at least once a year) to ensure they, and the questions they contain, are fit for purpose. Predictability of questions may also be reduced by providing a bank of questions that will be randomly assigned and refreshed every year.

Required supporting material

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

- a test specification
- sample test and mark scheme
- live test and mark scheme
- analysis reports which show areas of weakness for completed 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: Scenario Demonstrations with questioning

KSBs	Fail	Pass Descriptors should be in accordance with organisational policies and procedures
K8, K9, K11, S2, S5, S6, S9, S10, B4	Does not meet the pass criteria	Undertakes cyber security administrative operational tasks in accordance with security controls and procedures. Implements a technical cyber security control where cryptography and certificate management is required showing that the control is in place and performing the required function. Reviews and modifies access control requests from both internal and external stakeholders for modified rights to a digital information system. Conforms to the requirements for confidentiality, integrity and availability and demonstrates that the modified access controls are in operation.
K15, S11, S12	Does not meet the pass criteria	Scopes a cyber security vulnerability assessment taking into account organisational cyber security policies, procedures and standards, and produces the documentation required in order for a cyber security vulnerability assessment to be conducted. Reviews and evaluates the results of a cyber security vulnerability assessment and assesses the potential impact. Provides recommendations based upon the results of the evaluation.
K10, K19, S7, S16, S17	Does not meet the pass criteria	Monitors, identifies and describes information security events. Responds and reports whilst preserving the chain of evidence. Documents the incident according to standard procedures and follows procedures to ensure any learning from the incident is recorded. Demonstrates the drafting of reports using standard procedures.
K12, K16, K27, S13, S14, S15	Does not meet the pass criteria	Conducts a risk assessment, informed by gathering threat intelligence from external sources and network reconnaissance.

		Identifies and categorises sources of threats and risk. Identifies the business impact and at least one appropriate mitigation for management of each risk. Conducts maintenance of a digital information asset inventory by adding or removing an asset. Explains the process to securely dispose of an information asset.

Assessment method 2: Professional Discussion underpinned by Portfolio

KSBs	Fail	Pass	Distinction **The apprentice must meet 3 out of the 7 distinction criteria.**
K2, K20, K26, S1, S8, S18, B2, B3	Does not meet the pass criteria	Explains the main components of the organisation's information security policies and how they have employed them in practice and the outcome achieved. Explains organisational cyber security policies, procedures, standards and guidelines, including changes that may need to be made. Describes how to evaluate a service desk request and explains how and why they would escalate and when they have reached the limits of their authority for action. Describes how they have used a structured approach to prioritising the tasks. Describes the appropriateness of the authority level that they have and provides an example of when they have had to consider this.	Justifies why cyber security policies and procedures need to be reviewed and possibly amended on a regular basis given the continually changing nature of the cyber security threat landscape. Explain how amendments should be implemented in a managed way with reference to the need for version control.
K5, K22 K25, K29, K30, S3, S4, S22,	Does not meet the	Describes the cyber security culture and the ethical use of data within their organisation, the effectiveness of any existing cyber	Evaluates how and why their organisation's cyber security awareness programme can be improved and provides an example

B1, B5, B6	pass criteria	security awareness programme and how it is monitored. Explains the consequences of poor security awareness within their organisation and the wider society. Describes the impact that corporate cyber security culture has on customers and other stakeholders including brand and customer relationships. Explains the effect that this could have on the business and the approaches, such as training, that could be deployed to mitigate this if needed. Explains how they have contributed to the development of information security awareness training and how this has impacted on their organisation. Describes how they have met stakeholder expectations and deadlines. Describes how they have acted in line with occupation specific laws, regulations and professional standards and not accepted instruction that is incompatible with any of these. Explains how they have kept up to date with industry standards and recent legislation relating to cyber security. Establishes working relationships with co-workers and stakeholders which reflect the policies and procedures of the organisation.	of an improvement they have implemented.
K23, K24, K28, S21, B7	Does not meet the pass criteria	Explains how they keep up to date with changes in the cyber security industry and describes a recent development that is relevant to the organisation, and whether it has an impact upon their role. Explains how they review own development needs.	Evaluates how they plan to develop their skills further giving examples of specific activities they plan to undertake with reference to using one or more professional body skills framework(s).
K1, K13,	Does not meet the	Describes the major components of their organisation's Information	Evaluates how an Information Security Management System can

	pass criteria	Security Management System, why those components are important, and their role in reporting to management on the compliance and resilience of the business. Explains the principles and components of organisational information security governance. Explains disaster prevention and recovery methods.	assist in providing resilience to their organisation.
K6, K21, S19, S20	Does not meet the pass criteria	Explains how they have conducted a compliance check and how this supports cyber security audit requirements. Explains the principles of cyber compliance and monitoring. Explains cyber security audit requirements, procedures and plans. Explains effective use of cyber security compliance checks. Explains the translation of audit requirements and the collation of information.	Explains the steps that would need to be followed to achieve cyber compliance and implement a continual monitoring process within a team or business unit. Reviews and justifies cyber security compliance checks against the principles and policies of the organisation.

Assessment method 3: Knowledge Test

The following grade boundaries apply to the test:

Grade	Minimum score	Maximum score
Pass	25	40
Fail	0	24

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:

Scenario Demonstrations with questioning	Professional Discussion underpinned by portfolio	Knowledge Test	Overall grading
Fail	Any grade	Any grade	Fail
Any grade	Fail	Any grade	Fail
Any grade	Any grade	Fail	Fail
Pass	Pass	Pass	Pass
Pass	Distinction	Pass	Distinction
Fail	Pass	Fail	Fail

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

Apprentices should have a supportive action plan to prepare for the re-sit or a re-take. The apprentice's employer will need to agree that either a re-sit or re-take is an appropriate course of action.

An apprentice who fails an assessment method, and therefore the EPA in the first instance, will be required to re-sit or re-take just the assessment method failed. If the Knowledge Test is failed, then the apprentice will be given a different knowledge Test for the resit / retake.

Any assessment method re-sit or re-take must be taken during the maximum EPA period, otherwise the entire EPA must be taken again, unless in the opinion of the EPAO exceptional circumstances apply outside the control of the apprentice or their employer.

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

Where any assessment method has to be re-sat or re-taken, the apprentice will be awarded a maximum EPA grade of distinction, unless the EPAO determines there are exceptional circumstances requiring a re-sit or re-take.

Roles and responsibilities

Role	Responsibility
Apprentice	As a minimum the apprentice should: • complete the on-programme element of the apprenticeship • participate in development opportunities to improve their knowledge skills and behaviours as outlined in the standard • meet all gateway requirements when advised by the employer • understand the purpose and importance of EPA • prepare for and complete the EPA

Employer	As a minimum, the employer should: • support the apprentice to achieve the KSBs outlined in the standard to their best ability • determines when the apprentice is working at or above the level outlined in the standard and is ready for EPA • select the EPAO • confirm arrangements with EPAO for the EPA (who, when, where) in a timely manner • ensure apprentice is well prepared for the EPA • should not be involved in the delivery of the EPA
EPAO	As a minimum EPAOs should: • understand the occupational role • appoint independent assessors who have recent relevant experience of the occupation/sector at least one level above the apprentice gained in the last three years or significant experience of the occupation/sector • appoint independent assessors who are competent to deliver the end-point assessment in the occupation covered by this standard • provide training for independent assessors in terms of good assessment practice, operating the assessment tools and grading • have robust quality assurance systems and procedures that support fair, reliable and consistent assessment across the organisation and over time • operate induction training for independent assessors when they begin working for the EPAO on this standard and before they deliver an updated assessment method for the first time • deliver annual standardisation events for independent assessors. • appoint administrators/invigilators and markers to administer/invigilate and mark the EPA • provide training and CPD to the independent assessors they employ to undertake the EPA • provide adequate information, advice and guidance documentation to enable apprentices, employers and providers to prepare for the EPA • deliver the end-point assessment outlined in this EPA plan in a timely manner • prepare and provide all required material and resources required for delivery of the EPA in-line with best practices • use appropriate assessment recording documentation to ensure a clear and auditable mechanism for providing assessment decision feedback to the apprentice • have no direct connection with the apprentice, their employer or training provider i.e. there must be no conflict of interest

	• maintain robust internal quality assurance (IQA) procedures and processes, and conduct these on a regular basis • conform to the requirements of the nominated external quality assurance body • organise standardisation events and activities in accordance with this plan's IQA section • organise and conduct moderation of independent assessors' marking in accordance with this plan • have, and operate, an appeals process • arrange for certification with the relevant training provider • have processes in place to conduct internal quality assurance and do this on a regular basis
Independent assessor	As a minimum an independent assessor should: • understand the standard and assessment plan • deliver the end-point assessment in-line with the EPA plan • comply to the IQA requirements of the EPAO • be independent of the apprentice, their employer and training provider(s) i.e. there must be no conflict of interest • satisfy the criteria outlined in this EPA plan • hold or be working towards an independent assessor qualification e.g. A1 and have had training from their EPAO in terms of good assessment practice, operating the assessment tools and grading • have the capability to assess the apprentice at this level • attend the required number of EPAOs standardisation and training events per year (as defined in the IQA section) • be independent of the apprentice, their employer and training provider(s) i.e. there must be no conflict of interest • maintain a relevant cyber security qualification or have the equivalent experience of working at or above the level of this standard • are working currently as a practicing cyber security professional at level 4 or above and have experience of working in the information security industry for the last three years • are competent to assess the EPA • maintain an in-depth knowledge of the EPA and the grading criteria required, evidenced through CPD and assessor training • are committed to upholding the integrity of the Standard • have training at a sufficient depth to be effective and reliable when verifying judgements about assessment processes and decisions • have access to, and be engaging with, continuous professional development in order to keep up to date with industry • ideally be a member of a relevant professional body related to the standard
Training provider	As a minimum the training provider should: • work with the employer to ensure that the apprentice is given the opportunities to develop the KSBs outlined in the standard and monitor their progress during the on-programme period

	• advise the employer, upon request, on the apprentice's readiness for EPA prior to the gateway • play no part in the EPA itself

Internal Quality Assurance (IQA)

Internal quality assurance refers to the requirements that EPA organisations must have in place to ensure consistent (reliable) and accurate (valid) assessment decisions. EPA organisations for this EPA must:

- appoint independent assessors who have knowledge of the following occupational areas:
  - working as a practicing cyber security professional at level 4 or above with experience of working in the industry for the last three years in an information security role
- appoint independent assessors who are competent to deliver the end-point assessment
- provide training for independent assessors in terms of good assessment practice, operating the assessment tools and grading
- have robust quality assurance systems and procedures that support fair, reliable and consistent assessment across the organisation and over time
- operate induction training and standardisation events for independent assessors when they begin working for the EPAO on this standard and before they deliver an updated assessment method for the first time
- ensure independent assessors attend standardisation events on an ongoing basis and at least once per year for this occupational standard.

Affordability

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

- using an employer's premises
- assessing multiple apprentices simultaneously

Professional body recognition

This apprenticeship is designed to prepare successful apprentices to meet the requirements for registration as follows:

BCS - The Chartered Institute for IT / Associate BCS membership (AMBCS) and Professional Registration for IT Technicians (RITTech)

Chartered Institute for Information Security / Accredited Affiliate.

Mapping of knowledge, skills and behaviours (KSBs)

Assessment method 1: Scenario Demonstrations with questioning

Knowledge
K8 Common security administrative operational tasks e.g. patching, software updates, access control, configuring a range of firewalls, security incident and event management tools (SIEM) and protection tools (Anti-virus, Anti-malware, Anti-spam)
K9 Cryptography, certificates and use of certificate management tools
K10 Processes for detecting, reporting, assessing, responding to, dealing with and learning from information security events
K11 Principles of identity and access management - authentication, authorisation and federation - and the inter-relationship between privacy and access rights and access control, and the types of access control, access control mechanisms and application control
K12 Types of digital information assets used in a controlled environment and the need to maintain an inventory of information assets used in a controlled environment and the need for and practice of secure information asset disposal
K15 Components of a vulnerability assessment scope and techniques to evaluate the results of a vulnerability assessment and provide recommendations based upon the evidence provided by the vulnerability assessment tools. The impact that vulnerabilities might have on an organisation and common vulnerability assessment tools and their strengths and weaknesses
K16 Threat sources and threat identification and network reconnaissance techniques and the impact that threats might have on an organisation
K19 Standard information security event incident, exception and management reporting requirements and how to document incident and event information as part of a chain or evidence
K27 Risk assessment, risk management and business impact analysis principles

Skills
S2 Maintain information security controls
S5 Handle and assess the validity of security requests from a range of internal and external stakeholders
S6 Follow technical procedures to install and maintain technical security controls
S7 Monitor and report information security events
S9 Review and modify access rights to digital information systems, services, devices or data
S10 Maintain an inventory of digital information systems, services, devices and data storage
S11 Scope cyber security vulnerability assessments

S12 Evaluate the results of a cyber security vulnerability assessment
S13 Perform routine threat intelligence gathering tasks through consulting external sources
S14 Undertake digital information risk assessments
S15 Identify and categorise threats, vulnerabilities and risks in preparation for response or escalation
S16 Document cyber security event information whilst preserving evidence
S17 Draft information management reports using standard formats appropriate to the recipients

Behaviours
B4 A structured approach to the prioritisation of tasks

Assessment method 2: Professional Discussion underpinned by Portfolio

Knowledge
K1 Principles of organisational information security governance and the components of an organisation's cyber security technical infrastructure including hardware, operating systems, networks, software and cloud
K2 Cyber security policies and standards based on an Information Security Management System (ISMS)
K5 Cyber security awareness and components of an effective security culture, different organisational structures and cultures, the importance of maintaining privacy and confidentiality of an organisation's information and the impact of a poor security culture
K6 Principles of cyber security compliance and compliance monitoring techniques
K13 Disaster prevention and recovery methods and the need for continuity of service planning and how an organisation might implement basic disaster prevention and recovery practices using conventional and incremental secure backup and recovery techniques and tools both onsite and offsite including geographic considerations
K20 Common information security policies – acceptable use, incident management, patching, anti-virus, BYOD, access control, social media, password, data handling and data classification, IT asset disposal
K21 Cyber security audit requirements, procedures and plans, need to obtain and document evidence in an appropriate form for an internal or external auditor to review
K22 The significance of customer issues, problems, business value, brand awareness, cultural awareness/ diversity, accessibility, internal/ external audience, level of technical knowledge and profile in a business context
K23 Evolving cyber security issues in the digital world including the application to critical national infrastructure, communications technologies, the need for information assurance and governance, control systems and internet of things (IoT)

K24 Different learning techniques and the breadth and sources of knowledge and sources of verified information and data
K25 Importance of maintaining privacy and confidentiality of an organisation's information and the impact of a poor security culture
K26 Concepts of service desk delivery and how to respond to requests for assistance received by a service desk and be able to describe different methods of escalation, when to escalate to a higher level where necessary and the need to communicate accurately and appropriately during an escalation
K28 How their occupation fits into the wider digital landscape and any current or future regulatory requirements
K29 How to use data ethically and the implications for wider society, with respect to the use of data
K30 Roles within a multidisciplinary team and the interfaces with other areas of an organisation

Skills
S1 Follow information security procedures
S3 Develop information security training and awareness resources
S4 Monitor the effectiveness of information security training and awareness
S8 Recognise when to escalate information security events
S18 Review and comment upon cyber security policies, procedures, standards and guidelines
S19 Perform cyber security compliance checks
S20 Translate audit requirements and collate relevant information from log files, incident reports and other data sources
S21 Communication skills to co-operate as part of a multi-functional, multi-disciplinary team using a range of technical and non-technical language to provide an effective interface between internal or external users and suppliers
S22 Keep up to date with legislation and industry standards related to the implementation of cyber security in an organisation

Behaviours
B1 Manage own time to meet deadlines and manage stakeholder expectations
B2 Work independently and take responsibility for own actions within the occupation
B3 Use own initiative
B5 Treat colleagues and external stakeholders fairly and with respect without bias or discrimination
B6 Act in accordance with occupation specific laws, regulations and professional standards and not accept instruction that is incompatible with any of these
B7 Review own development needs in order to keep up to date with evolution in technologies, trends and innovation using a range of sources

Assessment method 3: Knowledge Test

Knowledge
K3 Types of physical, procedural and technical controls
K4 Awareness of how current legislation relates to or impacts upon the occupation including Data Protection Act, Regulation of Investigatory Powers Act, Human Rights Act, Computer Misuse Act, Freedom of Information Act, Official Secrets Act, Payment Card Industry Data Security Standard (PCI-DSS), Wireless and Telegraphy Act, professional body codes of conduct, ethical use of information assets
K7 Core terminology of cyber security – confidentiality, integrity, availability (the CIA triad), assurance, authenticity, identification, authentication, authorization, accountability, reliability, non-repudiation, access control
K14 Categories of cyber security vulnerabilities and common vulnerability exposures – software misconfiguration, sensitive data exposure, injection vulnerabilities, using components with known vulnerabilities, insufficient logging and monitoring, broken access control and authentication, security misconfiguration, incorrect cross-site validation
K17 Types of information security events – brute force attack, malware activity, suspicious user behaviour, suspicious device behaviour, unauthorized system changes
K18 Computer forensic principles – the importance of ensuring that evidence is not contaminated and maintaining the continuity of evidence without compromising it