Learn. To Change.

Level 4 Cyber Security Technologist

EPA Overview

July 2024

Contents

1. EPA headlines 1
2. Gateway 1
3. End Point Assessment 1
   Assessment Method 1: Professional Discussion underpinned by Portfolio 2
   Assessment Method 2: Scenario Demonstrations with Questioning 2
   Assessment Method 3: Project Report 3
   Assessment Method 4: Knowledge Test 4
4. Grading 4
5. Resit and Retakes 5

1.EPA headlines

- Must be on programme at least 366 days before entering gateway.
- Must have Portfolio, Project brief, declaration, Maths and English prior to gateway submission.
- Project Brief document (Gateway) – Max 500 words +/- 10%
- EPA period starts once EPAO approves Project Brief.
- EPA window is 3 – 6 months if a resit is required.
- 4 assessment methods at EPA –1. Professional discussion with underpinning portfolio, 2. Scenario demonstration, 3 Project report 4 Knowledge test.
- Professional discussion Lasts 90 Mins with a minimum of 12 open ended questions.
- Project report to be completed in 6 weeks from day of EPAO approval with a max word count of 2000 words +/- 10%.
- Scenario demonstration conducted over 7.5 hours over a 2-day period.
- Scenario demonstration questioning will last 45 mins.
- Knowledge test is 40 multi choice questions maximum 60 minutes to complete.

2. Gateway

Gateway is the point that the employer is satisfied that the apprentice is consistently working at or above the level set out in the occupational standard. In making this decision, the employer may take advice from the training provider, but the decision must ultimately be made by the employer.

Apprentices must have been programme for at least 366 days prior to entering gateway, and must also meet the following gateway requirements for Level 4 Cyber Security Technologist programme:

- Portfolio of evidence
- Portfolio checklist
- Portfolio declaration of authenticity
- Project Brief
- EPA gateway form
- Employer declaration
- Level 2 English and Maths evidence

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

3. End Point Assessment

The EPA window for Level 4 Cyber Security Technologist is typically 4 months but may be extended to a maximum of 6 months if an apprentice is required to resit or retake any assessment(s).

For the End Point Assessment, the learner must complete the following assessments:

- Assessment method 1: Professional Discussion underpinned by Portfolio
- Assessment method 2: Scenario Demonstrations with Questioning
- Assessment method 3: Project Report
- Assessment method 4: Knowledge Test

Assessment Method 1: Professional Discussion underpinned by Portfolio

The Professional Discussion underpinned by Portfolio assessment is graded Pass, Distinction or Fail.

The professional discussion is carried out with an Independent Assessor sourced by the EPAO. The professional discussion will last 90 minutes, with a discretionary 10% additional time to allow the apprentice to complete their last answer. The apprentice will be asked a minimum of 12 open questions based on the knowledge, skills, and behaviours identified for this assessment method., including at least 2 questions focused on 'law & regulation' (K8) and 1 question on 'ethics' (K9)

The portfolio will be compiled by the learner whilst on programme and should relate to the KSBs for this assessment. The portfolio underpins the professional discussion but is not directly assessed and therefore will not be marked. A copy of the portfolio must be available to the apprentice during the professional discussion.

Assessment Method 2: Scenario Demonstrations with Questioning

The Scenario Demonstrations with Questioning assessment is graded Pass, Distinction or Fail. This assessment has 2 components.

Component 1: Scenario Demonstrations

Apprentices will complete 4 scenario demonstrations in which they will demonstrate the knowledge, skills, and behaviours assigned to this assessment method. This assessment will be carried out over a total of 7 hours and 45 minutes, over 2 consecutive working days. Once a scenario demonstration has been started it must be completed on the same day to ensure the security of the assessment.

Prior to the assessment, the apprentice will 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.

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

The following activities must be observed during the scenario demonstrations:

Scenario 1 – Attack and Threat Research

- 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

- 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

- 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

- 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

Component 2: Questioning

The scenario demonstration questioning is carried out with an Independent Assessor sourced by the EPAO. The questioning will last 45 minutes, with a discretionary 10% additional time to allow the apprentice to complete their last answer. The apprentice will be asked a minimum of 9 questions based on the knowledge, skills, and behaviours identified for this assessment method.

The Independent Assessor will have a minimum of one week to review the scenario demonstration outputs ahead of the questioning assessment. During the questioning assessment apprentices will be provided with a copy of the outputs from their scenario demonstrations.

Assessment Method 3: Project Report

The Project Report assessment is graded Pass, Distinction or Fail.

The project is compiled after the apprentice has gone through the gateway process. Apprentices will conduct a project and deliver the outcome in the form of an electronic based report, which must be submitted to the EPAO after a maximum of 6 weeks of the EPA start date, which is once the project brief, has been approved by the EPAO assessor.

The employer must ensure the apprentice has sufficient time and the necessary resources, within this period, to plan and undertake the project and write the report. Whilst completing the project, the apprentice should be subject to normal workplace supervision.

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.

The project may be based on any of the following:

- A specific problem
- A recurring issue
- An idea/opportunity

As a minimum all project reports 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 has a maximum word limit of 2,000. A tolerance of plus or minus 10% is allowed. Appendices, references, diagrams etc will not be included in this total. The project must map, in an appendix, how it evidences the relevant KSBs for this assessment method.

Assessment Method 4: Knowledge Test

The knowledge test will consist of 40 multiple-choice questions. The multiple-choice questions will have four options of which one will be correct. Apprentices will have a maximum of 60 minutes to complete an online knowledge test, which maps to the knowledge requirements for this assessment method.

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

4. Grading

Professional Discussion underpinned by Portfolio	Scenario Demonstrations with Questioning	Project Report	Knowledge Test	Final Grade
Fail	Any grade	Any grade	Any grade	**Fail**
Any grade	Fail	Any grade	Any grade	**Fail**
Any grade	Any grade	Fail	Any grade	**Fail**

Any grade	Any grade	Any grade	Fail	**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**

5. Resit and Retakes

Apprentices who fail one or more assessment method will be offered the opportunity to take a resit or a retake at the employer's discretion. The employer will need to agree that either a resit or retake is an appropriate course of action. A resit does not require further learning, whereas a retake does.

Apprentices will have a supportive action plan to prepare for a resit or a retake of any failed assessment. All assessments must be successfully completed within the maximum EPA window, otherwise the full EPA will need to be resat or retaken.

Where any assessment method must be resat or retaken, the apprentice will be awarded a maximum EPA grade of Distinction.

Further information on the Level 4 Cyber Security Technologist EPA can be found in the assessment plan. A full list of the Knowledge, Skills and Behaviours (KSBs) can be found on the Institute for Apprenticeships website here.

QA.com