Level 4 Cyber Security Technologist v1.1

Update Webinar

Housekeeping

This session is being recorded

The session is being recorded and will be sent to all attendees after the webinar.

Everyone is on mute

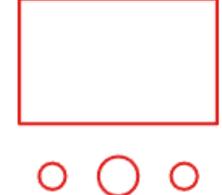To ensure the best experience for everyone, please keep your microphone muted.

Slides

The slides will be sent to all attendees alongside the recording after the webinar.

Questions

Please add your questions to the question function on the control panel. We will endeavour to answer all questions.

If the session cuts off

Please use the original webinar link to gain access back into the session. To join over the telephone, select "Phone Call" in the audio panel and the dial-in information will be displayed.

Agenda

1 The Standard

2 Preparing Gateway

3 Knowledge Test

4 Project Report

5 Professional Discussion underpinned by Portfolio

6 Scenario Demonstration with Questioning

7 Resources

8 Re-sits and Re-takes

9 Opportunities

10 Closing Slides

The Standard

The Occupational Role

The Occupational Role

The role of the cyber security technologist is essential in protecting organisations, systems, information, personal data and people from attacks and unauthorised access.

The primary role of the cyber security technologist is to use their knowledge of information security to deliver required cyber security outcomes that are effective and legally compliant. Cyber security technologists work in a variety of sectors and contexts. They may interact with internal and/or external stakeholders, developing and delivering solutions that fulfil the customer's requirements. The ability to interact effectively with people from a wide variety of roles and technical or non-technical skillsets is important in this occupation.

The work of a cyber security technologist encompasses specialist roles supporting business critical requirements and focuses on solutions that meet organisational needs. Tasks and project areas for this role may be technical, analytical, business or user focused. Cyber security technologists need to be able to take responsibility for their own work and collaborate successfully as part of a team that comprises different levels of technical and non-technical expertise.

Pathways

A **cyber security engineer** role is strongly technology focused. In their daily work, cyber security engineers will typically design, build and test secure networks or security products or systems with a particular focus on the security aspects of the design.

A **cyber risk analyst** focuses on risk assessment, analysis and providing advice on risk mitigations. Their role will also support formal security governance, regulatory & compliance (GRC).

A **cyber defender and responder** role is operationally focused. In their daily activities, a cyber defender and responder will typically configure and operate secure systems to prevent security breaches or monitor systems to detect and respond to security breaches.

Preparing for Gateway

Gateway Requirements

Gateway Requirements

The EPA period will only start when the **employer** is satisfied that the apprentice is consistently working at, or above the level of, the Standard. The apprentice must be able to evidence that they fully demonstrate the Occupational Standard and required level of professional competence in an authentic workplace context.

For the **Professional Discussion**, the apprentice is required to submit a Portfolio of Evidence, which must include a signed and dated 'Evidence Reference Matrix' form and a 'Declaration of Authenticity' form for the Portfolio

For the **Project Report**, the apprentice is required to submit a completed project brief (no longer than 500 words), using the ''Project Brief' form provided by City & Guilds or an approved alternative form.

The following should be completed on the EPA Pro platform:

- Gateway Declaration Form signed by the apprentice

- Gateway Declaration by the provider, on behalf of the employer and tutor – confirming that the apprentice has completed at least 12 months on-programme.

Gateway Requirements – Project Brief

City & Guilds will confirm when all the Gateway requirements have been met. The following requirements apply to the Project Brief and Project report:

- The proposed subject, title and scope of the project must be agreed between the provider/employer and City & Guilds immediately after Gateway. This will confirm the suitability of the proposed project before it is undertaken by the apprentice

- The IEPA will review and sign off the project brief within 2 weeks of the Gateway to ensure it has sufficient scope to meet the KSBs mapped to this method of assessment

- Should the project brief not be suitable, the IEPA will provide feedback to the apprentice so that the employer and apprentice can submit a revised project brief. Unless agreed otherwise with the City & Guilds End-point Assessment team, the employer and apprentice will have 5 working days from notification of rejection to submit a revised project brief

- It is important to note that the apprentice **cannot** start compiling the work-based project until the IEPA has formally accepted the project brief.

Knowledge Test

Assessment Method

Knowledge Test – Preparation

This assessment will take the form of an online multiple-choice test, delivered via City & Guild's e-volve platform. Entry for the test is made through the City & Guilds Walled Garden. The test will take place under controlled examination conditions. The test is 'closed book' which means that the apprentice **cannot** refer to reference books or materials during the assessment.

The provider and employer should prepare the apprentice for the knowledge test by carrying out formative tests throughout the on-programme period to test their knowledge and understanding of the Standard. This could include:

- Sharing the 9661 assessment specification as well as the occupational standard requirements found in this document

- Encouraging the apprentice to sit the City & Guilds sample knowledge tests under exam conditions. Sample tests are available on the website page for the 9661 EPA.

Knowledge Test – Grading and Timings

The knowledge test is a multiple choice exam. It is graded Pass/Fail. A maximum of 40 marks are available for the test. The test will be marked electronically by City & Guilds to generate your test score. To achieve a Pass, you must achieve a minimum of 25 marks.

There will be a maximum of 60 minutes to complete the test. The test will be carried out online via the e-volve platform. Each test question will have four options, of which only one will be correct. A correct response to a question is assigned one mark. An incorrect or missing answer is assigned zero marks.

Description	Coverage	Grade
Multiple choice test of knowledge-based questions, delivered online	K1, K13	P/X

Knowledge Test – Format

Section	Description
Time Allowed	60 minutes
# of Questions	40
Marks Available	40
Grading	P/X – minimum of 25 marks to achieve a **Pass**
Type of Questions	Multiple choice
Structure	20 Questions based on K1 20 Questions based on K13 Four options, of which **one** will be correct.
Marking	Test carried out online and marked electronically by City & Guilds

Project Report

Assessment Method

Project Report – Specification

The apprentice will conduct and submit a work-based project in the form of a Project Report. The Project Report will be marked and graded by the IEPA.

The aim of the project is to show evidence of how the apprentice has carried out work in response to a cyber security engineering issue. The activities carried out in the project must demonstrate work that reflects relevant practices for this role, meets the requirements of the employer organisation and allows the relevant KSBs to be demonstrated for this assessment method.

Since the project is work-based, the employer will provide an appropriate customer or other stakeholder specification from their day-to-day business activities. The employer will ensure the project has a real business application and has suitable coverage of the knowledge, skills and behaviours assigned to this assessment method. City & Guilds have provided an example of a project title and detailed guidance on the project requirements to enable the employer to select a suitable project that will meet the requirements of the EPA.

Project Report – Prior to Start

Prior to compiling the Project Report, the apprentice will scope out and deliver a **project brief** to City & Guilds at Gateway. The project brief is a summary of what the project will cover. The project brief:

- Should state the intended date that the work-based Project Report will be submitted to City & Guilds via the EPA Pro platform

- Should demonstrate that the proposed work-based project will provide sufficient opportunity for the apprentice to cover the KSBs assigned to this method

- Will outline the project plan, including an overview of

  - implementation stages/steps and associated timeframes

  - tasks contained within the project

  - the apprentice's responsibilities and duties for the project

- Is not assessed

- Should not be longer than **500 words**

- Should be submitted using the 'Project Brief' form provided in the Provider & Employer Recording Forms Pack. If the provider/employer intends to use their own version of the 'Project Brief' form, their form must be confirmed as suitable by City & Guilds before it is used.

Project Report – Requirements

The apprentice will conduct their project and submit their Project Report to City & Guilds within **a maximum of 6 weeks** after the EPA start date.

The Project Report should contain clear explanation of the tasks carried out and include acknowledgement of any sources used. The format and presentation of the Project Report is not prescribed, except for the following conditions which must be met:

- The Project Report must be submitted in the form of an electronic report

- Screenshots or extracts should be provided where reference to organisational documents is required

- Hyperlinks to external sources should not be used

- All the evidence submitted must be in a format that can be opened by the IEPA; where evidence cannot be opened, the Project Report will be returned without being reviewed.

The project should be based on a specification requiring the apprentice to respond to any of the following within the scope of their specialist role:

- A specific problem

- A recurring issue

- An idea/opportunity

Project Report – Cyber Security Engineer

The Project Report for the **cyber security engineer** must include the following:

- An introduction that consists of text only. Other formats such as diagrams, screenshots or figures must **not** be used in the introduction. The introduction should clearly set out:

  - a description of the project

  - the approach adopted

  - project outcomes and how the outcomes were achieved

  - the link between the project evidence and the KSBs assigned to this assessment method.

- Headings and evidence of tasks carried out for:

  - 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 meets the security requirements

  - demonstration of how the security features are effective.

Project Report – Cyber Risk Analyst

The Project Report for the **cyber risk analyst** must include the following:

- An introduction that consists of text only. Other formats such as diagrams, screenshots or figures must **not** be used in the introduction. The introduction should clearly set out:

  - a description of the project

  - the approach adopted

  - project outcomes and how the outcomes were achieved

  - the link between the project evidence and the KSBs assigned to this assessment method.

- Headings and evidence of tasks carried out for:

  - description of the role taken in a cyber security risk assessment and audit

  - a report explaining the conduct of the risk assessment and audit

  - a report considering the cyber policies and cyber awareness campaign.

Project Report – Cyber Defender and Responder

The Project Report for the **cyber defender and responder** must include the following:

- An introduction that consists of text only. Other formats such as diagrams, screenshots or figures must **not** be used in the introduction. The introduction should clearly set out:
  - a description of the project
  - the approach adopted
  - project outcomes and how the outcomes were achieved
  - the link between the project evidence and the KSBs assigned to this assessment method.
- Headings and evidence of tasks carried out for:
  - 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.
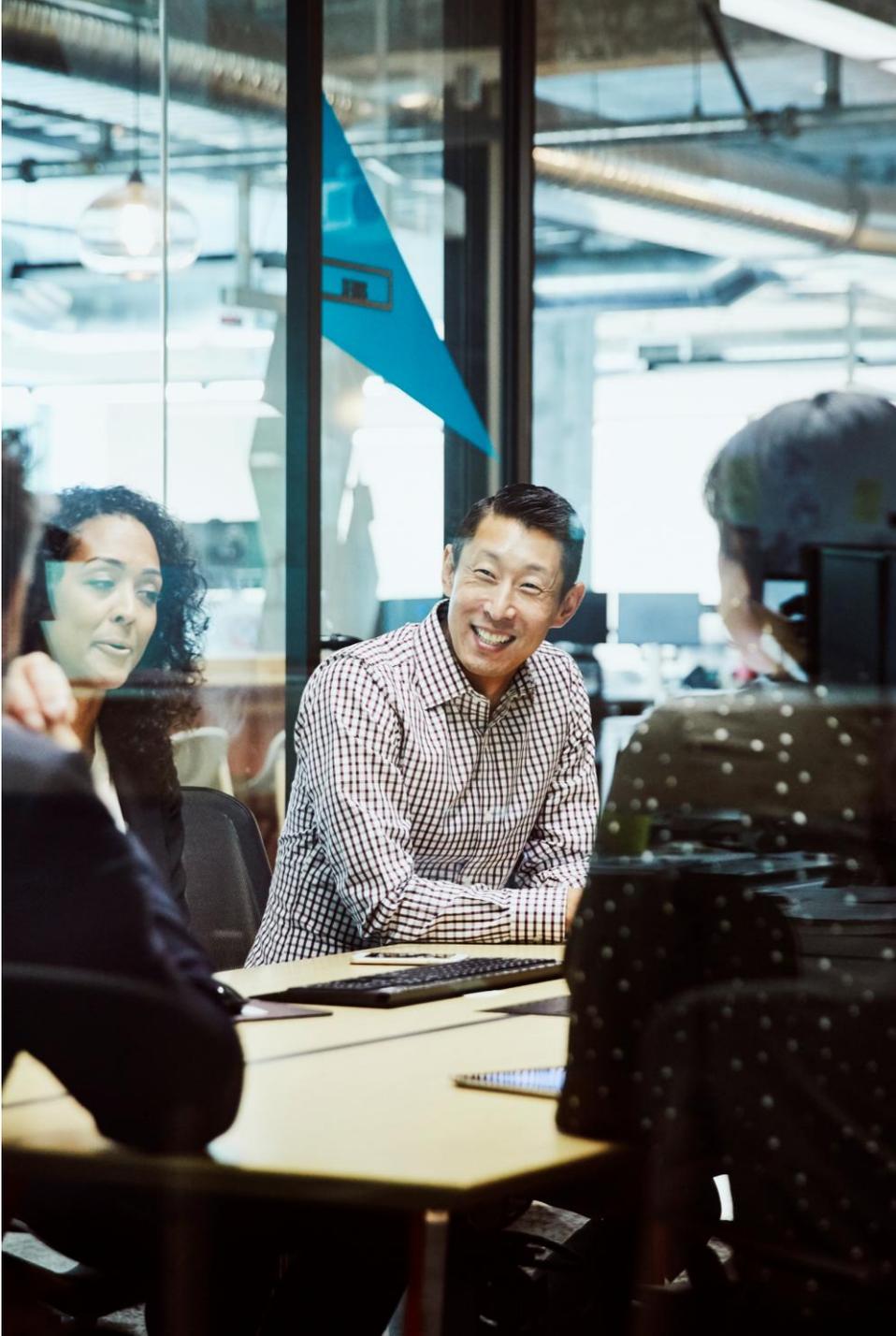
Project Report – Additional Information

The Project Report has a maximum word limit of **2000**. A tolerance of plus or minus 10% is allowed. Appendices, references, diagrams and/or video clips of up to 5 minutes in length will not be included in this total.

The project must map how it evidences the relevant KSBs for this assessment method. City & Guilds have provided an 'Evidence Reference Matrix' form in the *Provider & Employer Recording Forms Pack* for the apprentice to use for this assessment.

The submission of a fully completed 'Evidence Reference Matrix' form is mandatory. Failure to do so means that the IEPA will return the Project Report **without** it being reviewed.

The IEPA will review and mark the Project Report. The Project Report assessment will be graded Fail, Pass or Distinction. To pass the assessment method, the evidence presented in the Project Report must meet all the Pass criteria for the apprentice's chosen specialism. To achieve a Distinction, the evidence presented in the Project Report must meet all the Pass criteria and all the Distinction criteria for the apprentice's chosen specialism.

Professional Discussion underpinned by Portfolio

Assessment Method

Professional Discussion – Specification

This assessment will take the form of a Professional Discussion, which will be appropriately structured to draw out the best of the apprentice's competence and excellence.

The Professional Discussion will involve the questions that cover all the knowledge, skills and behaviours (KSBs) assigned to this assessment method and will consider the supporting evidence in the apprentice's Portfolio of Evidence. The two-way discussion will cover both what the apprentice has produced and how they have done it.

This assessment method makes use of naturally occurring evidence collated in the Portfolio of Evidence to support the assigned KSBs. It also allows for assessment of KSBs that do not occur on a predictable or regular basis or may not naturally occur during the Scenario Demonstrations or Project Report.

Professional Discussion – Requirements

The evidence in the Portfolio must be presented using these 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 and continuous improvement (S9, S15)

- Section 5: Following organisation's policies and processes (K6, S7)

- Section 6: Operation of security management systems & incident response (K7, K15)

Evidence may include:

- workplace documents, e.g. workplace policies, procedures and records

- photographic evidence with annotations

- video clips (maximum total duration 5 minutes); the apprentice must be in view and identifiable at all times

- witness statements or other employer contributions that focus on direct observation of performance rather than opinions

- Self-assessments must **not** be included as evidence

Professional Discussion – Evidence

Before selecting the evidence to form the Portfolio, the apprentice should consider the following:

- The grading descriptors and relevant KSBs to be covered by the Portfolio

- The type of evidence that can be presented (see Portfolio requirements above)

- The amount of evidence that should be presented

- The currency of evidence which must be produced while the apprentice is undertaking their apprenticeship.

To assemble the Portfolio, the apprentice should consider all the evidence they have available that shows they have met the requirements being assessed. From this, they should select evidence that most efficiently meets all the relevant grading descriptors and KSBs and which demonstrate their best performance.

There are two questions that an apprentice should consider when selecting work to form their portfolio:

1. Which pieces holistically (most efficiently) give evidence that together cover all of the relevant KSBs?

2. Is this the best evidence I have, showing that I have met all of the requirements for the higher grade?

Professional Discussion – Format

The Professional Discussion should be booked by the provider for the apprentice. The time and date of the Professional Discussion should be arranged with the City & Guilds End-point Assessment. The date may be booked through EPA Pro. The City & Guilds End-point Assessment team will assist in the booking process as required.

The IEPA will conduct and assess the Professional Discussion. It will last for **90 minutes**. The apprentice will be asked at least 12 questions.

These will include at least 2 questions focused on 'law & regulation' (K8) and 1 question on 'ethics' (K9).

The IEPA has the discretion to increase the time of the questioning by up to 10% to allow the apprentice to complete their last answer. Further time may be granted for apprentices with specific needs in line with the City & Guilds Reasonable Adjustment Policy.

The apprentice and the IEPA will have access to their own copies of the Portfolio throughout the Professional Discussion and both can refer to it as needed. The apprentice should draw on the contents of the Portfolio to underpin the discussion, selecting items to inform and enhance their answers.

27-Feb-26

Scenario Demonstration with Questioning

Assessment Method

Scenario Demonstration – Specification

The apprentice will complete 4 simulated Scenario Demonstrations provided online by City & Guilds. The Scenario Demonstrations will be followed by a Questioning session. Questioning will take place once the IEPA has reviewed the outputs of the 4 completed Scenario Demonstrations. The IEPA will require a minimum of 5 working days to review the Scenario Demonstration outputs.

The Scenario Demonstrations as well as the Questioning component must be completed within **10** working days, starting from the date when the apprentice undertakes their first Scenario Demonstration. The Scenario Demonstrations should usually be completed within 2 consecutive working days.

The aim of the Scenario Demonstrations is to show evidence of how the apprentice has carried out work in response to specified occupational tasks. The activities carried out in the tasks will reflect relevant working practices for this role and allow the apprentice to demonstrate the assigned knowledge, skills and behaviour (KSBs) for this assessment method.

The purpose of the IEPA Questioning will be to check the KSBs shown in the apprentice's Scenario Demonstrations and explore the underpinning reasoning and details of the evidence provided in the outputs of the Demonstration activities. The questions will focus on the outputs of each Scenario Demonstration and how these relate to the KSBs assigned to this assessment method.
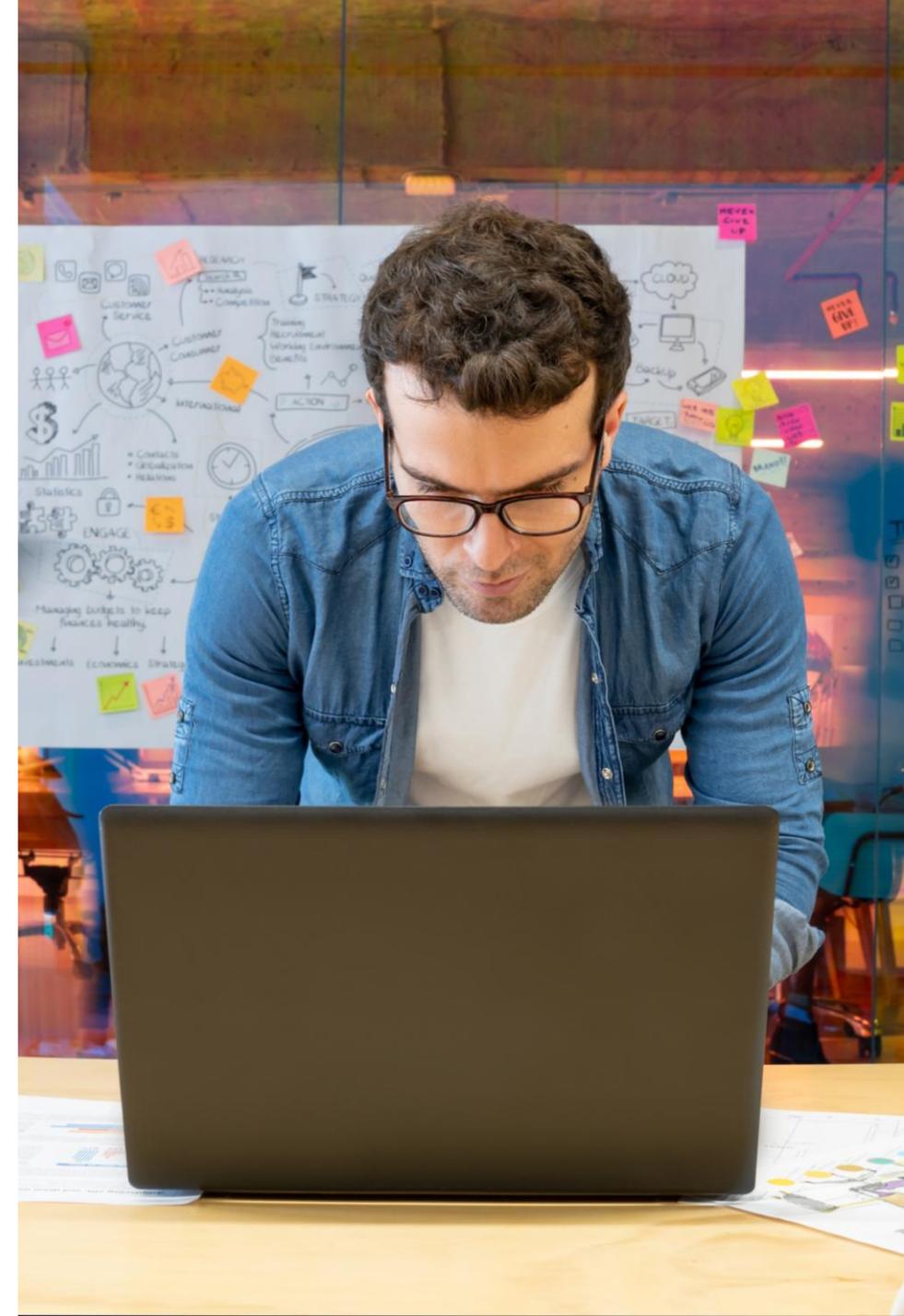
Scenario Demonstration – Structure

In **Scenario 1 – Attack and Threat Research** – the following must be covered:

- 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.

In **Scenario 2 – Risk Assessment** – the following must be covered:

- 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 Demonstration – Structure

In **Scenario 3 – Set up and configure a system with security features** – the following must be covered:

- 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.

In **Scenario 4 – Computer programme/script writing** – the following must be covered:

- 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

Scenario Demonstration – Timings

The following conditions apply to timings for the Scenario Demonstrations:

- The total time permitted for the completion of all the scenario demonstrations and production of evidence for the assessment tasks is 7 hours 45 minutes.

- The 7 hours 45 minutes are typically completed in a period of no longer than 2 consecutive working days

- A working day is typically considered to be 7.5 hours long

- Each of the 4 scenario demonstrations may not be split, other than to allow comfort breaks as necessary

- Once the apprentice has started a scenario demonstration, they must complete it on the same day; this is to ensure the security of the assessment

- Each Scenario Demonstration will be allocated the following amount of time for completion:

  – Attack and Threat Research scenario – 1 hour 45 minutes

  – Risk Assessment scenario – 2 hours

  – Set up and configure a system with security features scenario – 3 hours

  – Computer programme/script writing scenario – 1 hour.

Scenario Demonstration – Delivery

Prior to the start of the live assessment, City & Guilds will give the apprentice access to the simulated environment, background material, and guidance relating to the demonstration(s) that they will be carrying out. This will enable the apprentice to prepare for their assessment. At the beginning of their live assessment, the apprentice will be given access to the live area of the CloudShare environment. Once logged into CloudShare, the apprentice will receive clear instructions on the tasks they must complete, including timescales for completion. No additional clarification or guidance regarding the demonstration tasks may be provided by the responsible person, nor any other person.

The 4 scenarios do not have to follow immediately after each other. There is no need for the apprentice to complete the scenarios in any particular order.

After the Scenario Demonstrations are complete, the apprentice may **not** retain any materials created during the assessment, nor any copies of the scenario content that they used during the assessment.

Scenario Demonstration – Questioning

The IEPA must ask a minimum of **9 questions**, typically focused on scenarios 1 to 3, at their discretion. Follow up questions may be asked where clarification is required.

The Questions generated by the IEPA will focus on the outputs of the Scenario Demonstrations and the assigned KSBs.

During the Questioning component, apprentices must have a paper based or electronic copy of the outputs from their Scenario Demonstrations to refer to.

The Questioning session must last for **45 minutes**. Further time may be granted for apprentices with specific needs in line with the City & Guilds Reasonable Adjustment Policy.

The IEPA will decide how to allocate the available time for the Questioning across the 4 scenario outputs, based on where questions will add most value in increasing their understanding of the competence of the apprentice.

The IEPA has the discretion to increase the time of the Questioning by up to 10% to allow the apprentice to complete their answer to their final question.

Resources

EPA Pro and Support

Resources and Support

EPA Pro Resources include:

- EPA Pack

- EPA Resource List

- Guidance Documents (all Assessment Methods for Tutor/Apprentice)

- Sample Knowledge Test

- Sample Scenario Demonstration

- Sample Scenario Demonstration Appendix

- CloudShare Apprentice User Guide (also available as a YouTube link)

- EPA Hints and Tips

- LIEPA Report

- Recording Forms

Additionally, there is a Learner Preparation recording, walking

Apprentices through similar to what we have covered today.

CloudShare Apprentice User Guide

Using the Familiarisation and Sample Assessment Environment
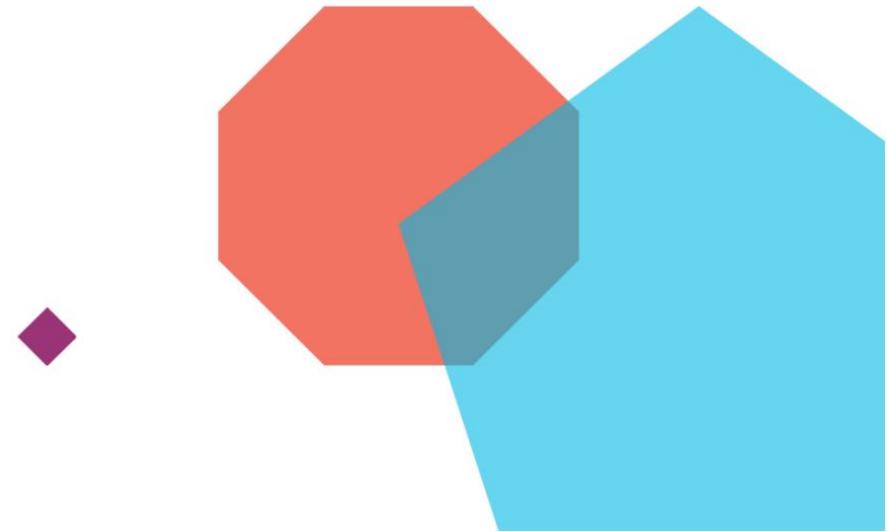
Re-sits and Re-takes

Guidance

Re-sits and Re-takes

Apprentices who fail one or more assessments will be offered the opportunity to take a re-sit or retake:

- A re-sit is where the apprentice takes the assessment again without the need for new learning. A re-take is where the employer determines new learning is needed first

- The employer must agree that either a re-sit or a re-take is appropriate course of action for the apprentice

- The provider and employer must ensure that a suitable action plan is put in place to support the apprentice in preparing for a re-sit or 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

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

- A re-sit should be taken within **8 weeks** of the Fail notification

- A re-take should be taken within **16 weeks** of the Fail notification

- Any assessment method re-sit or re-take must be taken within **24 weeks** of the Fail notification, otherwise the entire EPA must be taken again, unless, in the opinion of City & Guilds, exceptional circumstances apply outside the control of the apprentice or their employer.

Opportunities

Upcoming Works

Apprenticeship Reforms

As we progress through Apprenticeship Reforms, we are seeking insights on Reformed Assessment Plans to inform our developments.

Typically, we have run group or 1:1 sessions covering:

- Assessment Methods

- Assessment Timing

- Resource Requirements

- Concerns or Barriers

- Support Expectations

As each draft plan is released, we are scheduling meetings specific to that standard. If you wish to be included for specific, or all standards, register interest with the Technical Advisor.

Additional Information

Closing Slides

Associate Vacancies

We are looking for occupationally competent Independent End-point Assessors (IEPAs) and Lead Independent End-point Assessors (LIEPAs) to conduct End-point Assessments, as the apprentice completes their training.

Areas include (but not limited to):
- Information Communications Technician
- Cyber Security Technologist
- Data Technician
- Digital Support Technician
- Network Engineer
- Software Developer / Software Development Technician
- Multi-channel Marketer

Check out our Associate Vacancies site for Person Specifications, Task Profiles and How To Apply.

Home | City & Guilds Associate Vacancies (cityandguilds.com)

LinkedIn Group

We have a LinkedIn Group for all things Digital End-Point Assessment and Qualifications here at City & Guilds. We hope to continue to create a strong, supportive network with members from across centres, training providers and employers of all sizes. Asking questions and sharing of best practice is encouraged. The group will focus on information, resources and support for Qualifications and End-point Assessments.

To join, go to: https://lnkd.in/e94Dy3uP or scan the QR code below.

Contacts

City & Guilds supports providers through their Account Manager, EPA Partnership Managers, Customer Support and the Digital Sector team.

centresupport@cityandguilds.com
OR
general.enquiries@cityandguilds.com

Centre Support Number:
01924 930800
Learner Support Number:
01924 930801

Technical Advisor – Digital

david.mccallig@cityandguilds.com

Book time with me

Book Time

Keep up to date – register for email updates:
https://www.cityandguilds.com/what-we-offer/centres/email-updates

About City & Guilds

City & Guilds is the global skills partner, empowering people, organisations and economies to develop the skills they need for growth. With almost 150 years of trusted expertise, we support people into work, help them develop on the job and move into the next job.

We work with Governments, employers, training providers, colleges and industry stakeholders to design and deliver high-quality training, qualifications, assessments and credentials that lead to meaningful career progression. We understand the life changing link between skills development, social mobility and success. Our solutions span critical sectors including construction, engineering, transport, energy and electrical, serving over 1 million learners annually.

Through our comprehensive portfolio of brands and trusted global network, we set industry-wide standards for technical, behavioural and commercial skills to improve performance and productivity. We believe you can achieve your potential - and we're here to help make it happen.

Contact us

Giltspur House
5-6 Giltspur Street
London, EC1A 9DE

customersupport@cityandguilds.com

+44 (0) 1924 930 800

cityandguilds.com