Cyber Security Technical Professional Integrated Degree Apprenticeship

Level 6

End-Point Assessment Plan

INDEX

INTRODUCTION AND OVERVIEW

This plan sets out the requirements for end-point assessment (EPA) for the Cyber Security Technical Professional Integrated Degree Apprenticeship Standard. It is written for EPA Organisations (EPAOs) who need to know how EPAs for this apprenticeship must operate. It will also be of interest to apprentices, their employers and training providers.

The EPA starts after the Gateway has been passed.

This is an integrated degree apprenticeship, the degree cannot be awarded unless the apprenticeship is passed and vice versa.The EPA contributes 10 credits towards the degree and must be completed within three months of the Gateway.

The typical duration of the apprenticeship, including the EPA, is 48 months.

The EPA is conducted by a Lead Independent Assessor supported by a Second Independent Assessor. The EPAO is responsible for recruiting both assessors in accordance with the requierments of Section EIGHT of this plan. Independent assessors should be sourced from another University, industry, professional or other body; or if none of the above options are available the independent assessor can be from the same University but must be from a different department and independent of the apprentice's on-programme learning and assessment.

The Lead Independent Assessor will be assisted by a Second Independent Assessor who will contribute to assessing the EPA methods, but it is the Lead Independent Assessor who makes the final decision as to whether the apprentice has passed the EPA and the grade.

EPA tests all the skills, knowledge and behaviours (KSBs) on the Standard. It is based on two distinct assessment methods, both of which must passed in order for the apprentice to pass the apprenticeship.

The two EPA methods are:

(a) A Practical Test; and

(b) A Technical Discussion (informed by a portfolio).

The Independent Assessor will assess and grade the Practical Test and conduct, assess and grade the Technical Discussion. Following this, the Independent Assessor will determine whether the apprentice has passed or failed the apprenticeship overall and the grade achieved (fail, pass, merit or distinction). See Section Five (Grading) re the degree classification.

SECTION ONE: THE END-POINT ASSESSMENT GATEWAY

The EPA should only start once the Gateway requirements have been met and can be evidenced to the EPAO.

The Gateway requirements are that:

1. the employer confirms that the apprentice is ready for the EPA and has met the knowledge, skills and behaviour requirements set out in the occupational standard; and
2. the apprentice has completed and passed all the modules in the BSc Cyber Security Technical Professional degree; and

3. the apprentice has passed Level 2 English and maths (if not already achieved); and
4. the apprentice has produced a portfolio in relation to the KSBs for the Technical Discussion (see tables 1, 2, 3 and 4 below).

Portfolio requirements

The portfolio presents evidence from real-work projects and is used to help the apprentice answer questions in the Technical Discussion.

The portfolio will be created pre-Gateway and before EPA starts and is not assessed as part of the EPA. It contains evidence from projects that have been completed, usually, towards the end of the apprenticeship.

The portfolio is not marked as part of the EPA, but it does provide evidence that the Independent Assessor can use to probe further at the Technical Discussion.

Employers, with support from the HEI (as the apprenticeship delivery organisation), will assist the apprentice to assemble their portfolio.

The KSBs that are covered by the portfolio are as for Technical Discussion in tables 1, 2, 3 and 4.

The portfolio must be an e-portfolio presented digitally or online. It must include:

- a list of contents and a map of contents against the KSBs for the Technical Discussion as in tables 1, 2, 3 and 4; and
- a brief introduction/commentary by the apprentice, produced towards the end of their apprenticeship and highlighting, where appropriate, anything they would do differently; and
- evidence (see below) from between six and eight real work projects/pieces of work; and
- a testimonial from the employer, relating to the behavior shown in table 4; and
- written feedback from peers, colleagues and stakeholders; and
- demonstration of the business impact achieved during the apprenticeship; and
- evidence of teamworking; and
- a signed statement from the employer and HEI confirming this as being the apprentice's own work and confirming that, in their view, the work demonstrates the required KSBs as set out in tables 1, 2, 3 and 4 for the Technical Discussion; and
- a signed statement from the apprentice confirming this as her/his own work.

The portfolio may not include reflective accounts or self-evaluations.

The evidence referred to above can be submitted in a variety of appropriate and authentic formats, including:

- text, graphics, presentations, spreadsheets, project plans
- the product itself (such as a piece of code)
- job sheets, case studies, screen dumps, links
- photographs
- audio
- video
- written feedback

In terms of the employer testimonial referred to above (which is part of the portfolio), EPAOs should develop a template and/or guidance for employers to ensure the latter understand what EPAOs are looking for in a good portfolio.

The apprentice must provide the portfolio to the EPAO in at least one week before the commencement of the Technical Discussion.

SECTION TWO: END-POINT ASSESSMENT METHODS

Overview of End-Point Assessment Methods

Both the methods below must be passed.

Assessment Method	Areas Assessed	Assessed by	Grading
Practical Test	Apprentices undertake a Practical Test which consists of four exercises to be assessed against the defined set of KSBs (as set out in Tables 1, 2, 3 and 4 below) The Practical Test is undertaken in a controlled environment	Lead Independent Assessor from an EPAO from the Register of End-Point Assessment Organisations plus a Second Independent Assessor, also from the registered EPAO	Fail Pass Merit Distinction
Technical Discussion	Apprentices undertake a Technical Discussion which is assessed against the defined set of KSBs (as set out in Tables 1, 2, 3 and 4 below)	The same two Independent Assessors as above	Fail / Pass only

What is assessed in each assessment method?

The following tables shows each statement in the Standard, and which EPA method(s) tests it. The numbers in the table map to those on the Standard.

Table 1: Technical Competencies

	PRACTICAL TEST				TECHNICAL DISCUSSION
Technical Competencies	**Exercise 1**	**Exercise 2**	**Exercise 3**	**Exercise 4**	
1. Not applicable (knowledge only).					
2. Design, build, configure, optimise, test and troubleshoot simple and complex networks.	YES				
3. Apply statistical techniques to large data sets. Identify vulnerabilities in big data architectures and deployment.			YES		
4. Build test and debug a digital system to a specification.	YES				
5. Configure an Operating System in accordance with security policy. Identify threats and features.	YES				
6. Write, test, debug programs in high and low-level languages and scripts.				YES	
7. Design, implement and analyse algorithms.				YES	
8. Construct software to interact with the real world and analyse for security exploits.	YES				
9. Analyse malware & identify its mechanisms.		YES			
10. Apply secure programming principles and design patterns to address security issues.				YES	
11. Apply system engineering and software development methodologies and models.				YES	
12. Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations.		YES			
13. Assess culture & individual responsibilities.					YES
14. Undertake ethical system reconnaissance and intelligence analysis.			YES		
15. Undertake risk modelling, analysis and			YES		

trades.					
16. Undertake risk assessment to an external standard.			YES		
17. Apply a management system and develop an information security management plan.			YES		
18. Configure and use security technology components and key management.	YES				
19. Design & evaluate a system to a security case.	YES				
20. Architect, analyse & justify a secure system.	YES				YES
21. Develop an assurance strategy.		YES			YES
22. Security monitoring, analysis and intrusion detection. Recognise anomalies & behaviours.			YES		
23. Manage intrusion response, including with 3rd parties.			YES		
24. Not applicable (knowledge only).					
25. Organise testing & investigation work in accordance with legal & ethical requirements.		YES			
26. Develop & apply information security policy to implement legal or regulatory requirements.	YES				

Table 2: Technical Knowledge and Understanding

The numbers in the table map to those on the Standard.

	PRACTICAL TEST				TECHNICAL DISCUSSION
Technical Knowledge and Understanding	**Exercise 1**	**Exercise 2**	**Exercise 3**	**Exercise 4**	
1. Foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance.					YES
2. Network foundations, connections, internet working, protocols, standards, performance, security and server virtualisation.	YES				
3. Information management, big data concepts, statistical techniques, database concepts and data quality.			YES		
4. Computer architecture, digital logic, machine level representation of data.	YES				
5. Operating system principles, architectures, features, mechanisms, security features and exploits.	YES				
6. Algorithm and program design concepts, compilers and logic. Programming languages.				YES	
7. Algorithms, complexity and discrete maths.				YES	
8. How software interacts with hardware and real-world environment and security issues.	YES				
9. Malware, reverse engineering, obfuscation.		YES			
10. Defensive programming, malware resistance, code analysis, formal methods, good practice.				YES	
11. System development principles, tools, approaches, complexity, software engineering.				YES	
12. Threats, vulnerabilities, impacts and mitigations in ICT systems and the enterprise		YES			

environment.					
13. Human dimensions of cyber security.					YES
14. Structured and ethical intelligence analysis, methods and techniques.			YES		
15. Management of cyber risk, tools and techniques.			YES		
16. Quantitative and qualitative risk management theory & practice, role of risk stakeholders.			YES		
17. Concepts and benefits of security management systems, governance & international standards.			YES		
18. Security components: how they are used for security / business benefit. Crypto & key management.	YES				
19. How to compose a justified security case.	YES				
20. Understand security assurance, how to achieve it and how to apply security principles.	YES				YES
21. Assurance concepts & approaches.		YES			YES
22. How to diagnose cause from observables. Application of SIEM (Security Information and Event Management) tools & techniques.			YES		
23. Cyber incident response, management, escalation, investigation & 3rd party involvement.			YES		
24. Legal, regulatory, compliance & standards environment.					YES
25. Applicability of laws, regulations & ethical standards.		YES			
26. Legal responsibilities of system owners, users, employers, employees.	YES				

Table 3 Underpinning professional, interpersonal and business skills

Underpinning professional, interpersonal and business skills	PRACTICAL TEST (each exercise)	TECHNICAL DISCUSSION
Fluent in written communications and able to articulate complex issues.	YES	
Makes concise, engaging and well-structured verbal presentations, arguments and explanations.		YES
Able to deal with different, competing interests within and outside the organization with excellent negotiation skills.		YES
Able to identify the preferences, motivations, strengths and limitations of other people and apply these insights to work more effectively with and to motivate others.		YES
Able to work effectively with others to achieve a common goal.		YES
Competent in active listening and in leading, influencing and persuading others.		YES
Able to give and receive feedback constructively and incorporate it into his/her own development and life-long learning.		YES
Analytical and critical thinking skills for Technology Solutions development and can systematically analyse and apply structured problem-solving techniques to complex systems and situations.	YES	
Able to put forward, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business need, using open questions and summarising skills and basic negotiating skills.		YES
Can conduct effective research, using literature and other media.	YES	
Logical thinking and creative approach to problem solving.	YES	
Able to demonstrate a 'security mind-set' (how to break as well as make).	YES	

Table 4 Behaviours

Behaviours	PRACTICAL TEST (each exercise)	TECHNICAL DISCUSSION
Demonstrates business disciplines, ethics and courtesies, demonstrating timeliness and focus when faced with distractions and the ability to complete tasks to a deadline with high quality.	YES	
Flexible attitude and ability to perform under pressure.	YES	
A thorough approach to work in the cyber security role.		YES

The EPAOs should use the Tables above as the basis for a checklist for the Independent Assessor to use, to ensure the right KSBs are assessed in each method and to record where sufficient evidence has been demonstrated for each KSB.

SECTION THREE: THE PRACTICAL TEST

The Practical Test consists of four exercises:

- each exercise will take 12 hours +10% at the discretion of the Lead Independent Assessor to complete
- the whole Practical Test will take a 48 hours +-10% at the discretion of the Lead Independent Assessor to complete
- the whole Practical Test will be taken within a period of two weeks.

The Practical Test is designed to assess the apprentice in a consistent way, irrespective of their particular role in their company. The EPAO is responsible for sourcing a venue for the EPA.

EPAOs must develop 'practical specification 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.'

Each Practical Test (and its constituent four exercises) will present a typical business task, appropriate to an SME, an IT business, a large corporate or a non-IT business, and in the public and private sectors.

Each Practical Test will include the bundle of four exercises which will include a short summary. The EPAO will select the Practical Test the individual apprentice will take. The EPAO can ask the employer what the former needs to consider when selecting the Practical Test the individual apprentice will take.

Each Practical Test will balance the need to: 1) be specific to ensure consistency and comparability; and b) be sufficiently flexible to allow apprentices to apply the approaches in their job role.

EPAOs will test and trial the exercises with small groups of apprentices, employers and training providers. This will ensure they are valid, reliable and comparable to other exercises, before being implemented.

EPAOs will monitor the Practical Tests and the constituent exercises over time to ensure comparability and continued relevance.

Existing Practical Tests and their constituent exercises will be rotated and new ones introduced

The outputs of the exercises will be assessed by the Lead Independent Assessor (with input from the Second Independent Assessor) against the KSBs assigned to this method as shown in Tables 1, 2, 3 and 4, and a grade assigned using the descriptors in Annex. Although each exercise will test specified KSBs on the Standard, they will be grouped shown below.

Each exercise must be passed in order for the Practical Test as a whole to be passed. Grading is described in Section FIVE below.

<u>Outputs from Exercise One (Design for Security)</u>

1. A physical, designed network, plus software as set out in the KSBs listed in tables, 1,2, 3 and 4 above; and
2. A written justification for the approach taken (a 1,000 word +/- 100 words written document).

<u>Outputs from Exercise Two (Test for Security)</u>

1. A physical demonstration of a security test of a provided network as set out in the KSBs listed in tables 1,2, 3 and 4 above; and

2. A written justification for the approach taken (a 1,000 word +/- 100 words written document).

Outputs from Exercise Three (Monitor)

1. A physical demonstration of monitoring a provided network as set out in the KSBs listed in 1,2, 3 and 4 above; and

2. A written justification for the approach taken (a 1,000 word +/- 100 words written document).

Outputs from Exercise Four (Defensive Programming)

1. A defensive programme as set out in the KSBs listed in tables 1, 2, 3 and 4 above; and

2. A written justification for the approach taken (a 1,000 word +/- 100 words written document).

3A Practical arrangements

Apprentices will complete the Practical Test off-the-job, so that they are away from the day-to-day pressures of work and in a 'controlled' environment, which will be at the HEI premises.

Each of the exercises will have a detailed brief and instructions for the apprentice – and this will not be opened until the first morning of the first day in which the exercise in question is carried out.

Each exercise will specify what systems, tools and platforms will be required to complete the tasks.

3B The controlled environment

The controlled environment must:

- be a quiet room, away from the normal working environment - at the HEI's premises; and
- have a dedicated work station; and
- be away from disruptions; and
- provide access to all required equipment, tools, systems; and
- have very reliable internet access.

There may be others undertaking the same exercise at the same time, but they must be at least two meters apart, at separate workstations and with their own resource pack.

The EPAO is responsible for ensuring the controlled environment is appropriate including the local management arrangements. The EPAO must make arrangements for an invigilator to be present the whole time.

Work must be saved to the secure platform between work sessions – and backed up (note this partial work is not assessed although it is possible to check that the work that has been done has not changed between work sessions).

Reasonable adjustments must be made for apprentices who need them in line with normal EPAO procedures.

3C Assessment of the Practical Test

The outputs from the Practical Test are assessed by the two Independent Assessors and then the Lead Independent Assessor makes the judgement on grading against the grading descriptors in Annex 1.

The outputs are created during the Practical Test itself so the Independent Assessors have immediate access to those outputs which the apprentice leaves behind in the room in which the Practical Test takes place.

Independent Assessors are looking for sufficient evidence from the Practical Test to determine whether the minimum standard has been achieved for all the KSBs being assessed via this method.

The Practical Test is graded as fail, pass, merit or distinction.

SECTION FOUR: THE TECHNICAL DISCUSSION

The purpose of the Technical Discussion is to elicit sufficient evidence against the KSBs assigned to it (as shown in Tables 1, 2, 3 and 4) to inform whether the minimum standard has been achieved.

The Technical Discussion is graded as fail / pass only.

The Technical Discussion is informed by the outputs contained in the submitted portfolio.

4A Practical Requirements

The Technical Discussion is undertaken by the Lead Independent Assessor (the same one who assessed the Practical Test) but s/he will be assisted in the Technical Discussion by a Second Independent Assessor (the same one as assisted the Lead Independent Assessor in assessing the Practical Test). Both of them must be from a registered EPAO and neither of them can have had any role in the on-programme teaching of the apprentice in question. It is the Lead Independent Assessor who makes the grading decision, but with input from the Second Independent Assessor.

The Technical Discussion can be conducted either face-to-face (in a quiet room at the HEI's premises) or online.

The apprentice will have at least seven working days' notice of the date and time of the Technical Discussion and it will take place within the four-month EPA period.

The Technical Discussion should give the apprentice the best possible opportunity to demonstrate the KSBs being assessed via this method. The apprentice can use their portfolio to help answer the questions. The Lead Independent Assessor and the Second Independent Assessor should ask open questions to encourage the apprentice to illustrate the KSBs set out in tables 1, 2, 3 and 4.

The Technical Discussion will last 120 minutes +/- 10% at the discretion of the Lead Independent Assessor.

It is a structured Technical Discussion between the apprentice, the Lead Independent Assessor and the Second Independent Assessor. It assesses the KSBs assigned to it; it is NOT a test of their interview skills.

The Lead Independent Assessor and the Second Independent Assessor must put the apprentice at

their ease and give them the opportunity to do their very best.

Preparation for the Technical Discussion

The Lead Independent Assessor and the Second Independent Assessor will:

- remind themselves of the KSBs being tested via this method; and
- review (but not assess) the portfolio.

EPAOs will produce a structured brief for the Lead Independent Assessor and Second Independent Assessor to support the Technical Discussion and a bank of potential questions from which the Lead Independent Assessor can select the most appropriate. There will be a minimum of 16 questions.

EPAOs must develop 'banks of potential questions' 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.'

In addition the Lead Independent Assessor and Second Independent Assessor may ask follow up questions or prompts to elicit further information or more in-depth replies to each question, such as "tell me more about.." "tell me why you decided…".

After the Technical Discussion

The main points from the Technical Discussion, and the conclusions, will be documented by the Lead Independent Assessor during the Technical Discussion. The grading decision will be taken within 14 days of this.

The Technical Discussion will be recorded by the Lead Independent Assessor for internal and external moderation purposes.

Reasonable adjustments must be made for apprentices who need them in line with normal EPAO procedures.

4B Assessment of the Technical Discussion

The outputs from the Technical Discussion are assessed by the two Independent Assessors and then the Lead Independent Assessor makes the judgement on grading against the grading descriptors in Annex 2.

The Technical Discussion is graded as fail / pass only.

SECTION FIVE: GRADING

Table 5

Grade for the Practical Test	Definition
Fail	One or more of the KSBs tested have not met the pass criteria.

Pass	All the KSBs tested have met the pass criteria.
Merit	The Pass criteria have been met AND Technical Competencies and Technical Knowledge and Understanding numbers 2, 9, 10, 12, 15, 19 and 20 been demonstrated to at least Merit level
Distinction	The Merit criteria have been met AND Technical Competencies and Technical Knowledge and Understanding numbers 2, 9, 10, 12, 15, 19 and 20 have been demonstrated to Distinction level

The detail in the above table relates to the grade descriptors shown in Annex 1. The EPAO will ensure that the relevant grade descriptors for the technical competencies and knowledge for each of the four exercises described in Tables 1 and 2 above are taken into account when making the grading decision.

The purpose of grading is to differentiate between those apprentices whose work is at the minimum requirements for a pass and those whose work significantly exceeds this, and meets the requirements for a merit or a distinction.

The Lead Independent Assessor makes the final decision about whether the apprentice has passed and what grade they have achieved.

Based on the evidence they have assessed, the Lead Independent Assessor will determine if there is sufficient evidence to meet the minimum requirements and then whether there is sufficient evidence to demonstrate that the apprentice has significantly exceeded the requirements to achieve a merit or distinction.

Where the Lead Independent Assessor is unsure whether or not the apprentice has passed the apprenticeship or the grade because the apprentice is on the borderline, s/he may seek advice from whoever in the EPAO is responsible for the quality of assessment decisions.

Appeals on grading decisions should be investigated and resolved through the EPAO's formal and documented process, and records of such appeals should be retained.

Principles

An apprentice must pass both EPA methods in order to pass the apprenticeship overall.

The table below shows how an overall grade for the apprenticeship is achieved.

Table 6

Practical Test	Technical Discussion	Overall Grade
Pass	Pass	Pass
Merit	Pass	Merit
Distinction	Pass	Distinction

Grading process

Apprentices are informed, in writing, whether they have passed the Practical Test and the grade awarded before they take the Technical Discussion.

See below re re-takes and re-sits of the EPA methods.

At the end of the EPA, the apprentice is given the grade for the whole apprenticeship.

The final decision as to whether the apprentice has passed the EPA is made by the Lead Independent Assessor.

BSc Degree Grading

The degree will be classified in accordance with university integrated degree regulations. If an apprentice fails the EPA, the degree cannot be awarded and vice versa.

SECTION SIX: RE-SITS and RE-TAKES

Apprentices who fail one or more assessment methods may, depending upon their employers, be offered the opportunity to take a re-sit/re-take. A re-sit does not require further learning, whereas a re-take does. Re-sits/re-takes must not be offered to apprentices wishing to move from pass to distinction.

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

Both assessment methods must be successfully passed within 3 months of the gateway; otherwise the entire EPA must be re-sat/re-taken. There are no restrictions on the grade awarded in the case of a re-sit/re-take.

EPAOs must ensure that apprentices complete a different Practical Test and/or are asked different questions as part of the Technical Discussion when taking a re-sit/re-take.

SECTION SEVEN: PROFESSIONAL BODY RECOGNITION

This apprenticeship is recognised for entry to the Institute of Information Security Professionals at Associate level.

SECTION EIGHT: QUALITY ASSURANCE – INTERNAL

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

- develop and provide EPA guidance to apprentices, employers, on-programme HEI personnel and the independent assessor in relation to the EPA requirements
- ensure the apprentices, employers, on-programme HEI personnel and the independent assessor are all aware of the Technical Competencies, Technical Knowledge and understanding, Underpinning professional, interpersonal and business skills, and Behaviour

requirements (as set out in the Standard) and the grading criteria (as set out in this EPA Plan)

- develop compensatory assessment for learners with special requirements to allow reasonable adjustments to be made to assess the apprentice (for example, sign language support if necessary). Whilst these will remove barriers to participation, they must be designed to ensure judgements are not compromised to health and safety and legal requirements
- appoint the Lead Independent Assessor and the Second Independent Assessor and ensure they are competent to do the job (see criteria below) and understand the terms of the requirements of the operation and marking of assessment methods and in undertaking fair and impartial assessment
- monitor and provide support to the independent assessors where required to ensure consistent assessment
- develop and provide documentation for recording assessment decisions
- hold annual standardisation events for independent assessors to ensure consistent application of the guidance
- operate moderation of assessment activity and decisions at least annually, through examination of documentation and observation activity, with a minimum of 10% of each independent assessor's assessments moderated (or 5 moderations, whichever is the higher)
- provide immediate guidance where end-point assessments need to be halted due to unforeseen circumstances eg system emergency, apprentice illness
- ensure independent assessors undertake regular continuing professional development
- ensure independent assessors have the necessary skills and industry knowledge to make reliable judgements and to confirm that they have not been involved in any way in teaching the apprentice they are assessing whilst that apprentice was on the programme
- recruit the independent assessors who are competent in the occupation they are assessing, in terms of:

    - up-to-date, relevant, in-depth and broad experience of working in a cyber security role
    - relevant industry cyber security expertise equivalent to or higher than Level 7 and/or relevant professional recognition at a Level 7 or higher
    - the possession of practical and up to date knowledge of the application of current working practices, infrastructure, tools and technologies appropriate to cyber security roles

In addition, Independent Assessors must have completed an induction to demonstrate working knowledge of the apprenticeship standard and the assessment process. They must be fully trained and approved for use of each of the assessment tools and be trained in the consistent application of the grading criteria. They must attend standardisation meetings annually to ensure and maintain consistency of assessment decisions.

Anyone who undertakes end-point assessment must be held on a register by the registered EPAO. The register must confirm that each individual undertaking EPA has satisfied the criteria above and that the evidence has been checked through, for example a combination of:

- personal interviews
- qualifications
- CPD certificates
- employment history
- testimonials

- EPAO induction and training events

SECTION NINE: QUALITY ASSURANCE - EXTERNAL

The Institute for Apprenticeships is exploring whether QAA can undertake external quality assurance for this standard, and arrangements will be confirmed.

SECTION TEN: IMPLEMENTATION

Affordability: Costs will be kept down by requiring:

- the development of online approaches, including online materials, resources and assessment processes, to enable scalability and cost-effectiveness
- a pragmatic combination of assessment methods ensures breadth, validity and reliability to satisfy the assessment requirements whilst minimising additional, non-value adding assessment costs
- the simplification of roles and responsibilities in the assessment process

Consistency: all UK universities must follow the Quality Assurance Agency for High Education (QAA) code of practice for assurance of academic quality and standards in higher education.

Volumes: we estimate that there will be approximately 300 starts per annum on this integrated degree apprenticeship at steady state.

ANNEX 1: GRADE DESCRIPTORS FOR THE PRACTICAL TEST (Fail / Pass / Merit / Distinction)

An apprentice will fail the Practical Test if he/she has not met all of the pass criteria below.

Technical Competencies tested

The standard	Minimum for a pass. The apprentice can…	Merit: in addition to the pass requirement, the apprentice can…	Distinction: in addition to the pass and merit requirements, the apprentice can…
Technical Competency 2 (on the standard) Design, build, configure, optimise, test and troubleshoot simple and complex networks.	Design, build and test a simple network that includes hubs, switches, routers and user devices to a given design requirement without supervision. Provide evidence that the system meets the design requirement. Design, build & test a distributed network (more than 1 sub-net) with static and dynamic routes. Troubleshoot typical problems in network designs and implementations.	Provide evidence that the configured and optimised network meets the stated requirements. Show that they considered more than one option in terms of approach to designing the network.	Troubleshoot complex problems in network designs and implementations.
Technical Competency 3: apply statistical techniques to large data sets. Identify vulnerabilities in data architectures and deployment	Apply statistical techniques to large heterogeneous data sets to determine trends or anomalies as part of security analytics. Identify vulnerabilities in big data architectures. Design and set up database of relevant information. Use a declarative query language to elicit information from a database.	Not applicable.	Not applicable.

Technical Competency 4: Build, test and debug a digital system to a specification.	Build, test and debug a digital system employing a number of different components that works to achieve a defined specification.	Not applicable.	Not applicable.
Technical Competency 5: Configure an Operating System (OS) in accordance with security policy. Identify threats and features.	Identify potential threats to OSs and the security features designed to guard against them and residual vulnerabilities of these security features. Configure OSs according to security policies and integrate into system development.	Not applicable.	Not applicable.
Technical Competency 6: Write, test and debug programmes in high and low-level languages and scripts.	Write, test and debug a programme in a high-level language that works to achieve a defined specification. Design and implement solutions to problems using a variety of programming styles. Map between a high-level programming language expression and its low-level executable code. Design and implement simple solutions directly in an assembler language. Design and implement solutions using a scripting language.	Not applicable.	Not applicable.
Technical Competency 7: Design, implement and analyse algorithms.	Design, implement and analyse algorithms for solving problems.	Not applicable.	Not applicable.

Technical Competency 8: Construct software to interact with the real world and analyse for security exploits.	Construct a simple system to demonstrate software interacting with the physical world and analyse how the software-physical interactions may be exploited.	Not applicable.	Not applicable.
Technical Competency 9: Analyse malware & identify its mechanisms.	Analyse examples of malware and identify the mechanisms used by the malware.	Analyse malware which incorporates complex behaviours such as obfuscation and anti-reverse engineering.	Script / compose custom tool sets for the analysis of more complex malware.
Technical Competency 10: Apply secure programming principles and design patterns to address security issues.	Apply secure programming principles to analyse software designs and implementations to mitigate identified security vulnerabilities to produce more resilient code, with evidence. Apply secure design patterns and organisational coding standards in the development of a software solution.	Identify more subtle vulnerabilities in software codebase examples.	Develop mitigations to these vulnerabilities.
Technical Competency 11: Apply system engineering principles and software development methodology and models	Apply a systematic software development methodology, employing appropriate tools, to develop a solution that meets the needs of users and customers and that addresses the whole lifecycle. Create a system description of a complex system of interest including aspects of people, culture, technology and process in a defined environment. Use the system description to identify and analyse security aspects.	Not applicable.	Not applicable.

Technical Competency 12: Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations.	Discover through a mix of research and practical exploration vulnerabilities in a system and determine their impact. Research and investigate common and complex attack techniques including making use of relevant external sources of vulnerabilities, threat intelligence and advice. (For example. a national cyber authority, OWASP.) Combine different sources to create an enriched view. Demonstrate application of attack techniques in a lab setting (in a legal and ethical manner). .	Research, analyse and evaluate security threats and hazards to a specific system including technology and considering services or processes.	Devise mitigations to defend against security threats and hazards to a specific system including technology and considering services or processes.
Technical Competency 14: Undertake ethical system reconnaissance and intelligence analysis	Analyse multiple, potentially contradictory, sources of information, to identify patterns and hypothesise a likely picture, which can be supported by arguments and evidence based on the sources. Consider provenance of sources and how this affects the quality of evidence, arguments and conclusions. Use OSINT (Open-source Intelligence) to profile a defined target (organisation or system), and identify potential vulnerabilities (legally). Demonstrate an eye for detail and critical thinking ability.	Not applicable.	Not applicable.

Technical Competency 15: Undertake risk modelling, analysis and trades.	Relate cyber risk to other relevant classes of risk (business and operational risks) and perform costs analysis and present trade-off arguments in a business case, illustrating commercial or value for money judgement. Apply system modelling techniques to risk, vulnerability and impact in order to enable trade-offs and to inform risk analysis. (Employ a method such as SABSA, DBSy, CVSS scoring, STRIDE, NIST 800-154). Compose a system to create an architectural model for the purpose of risk assessment and integrate with an enterprise model.	Compare & contrast two system modelling techniques to risk, vulnerability and impact in order to enable trade-offs and to inform risk analysis. (Employ two methods from SABSA, DBSy, CVSS scoring, STRIDE, NIST 800-154). Compare and contrast the differences between the two techniques in terms of the effect on any subsequent risk analysis.	Ensure that, in comparing and contrasting techniques, options are identified for investment in measures to mitigate cyber risk based on analysis and modelling in an enterprise scenario.
Technical Competency 16: Undertake risk Assessment to an external standard.	Undertake a security risk assessment for a simple system without direct supervision and propose remediation advice in the context of the employer. Conduct a cyber-risk assessment against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.	Not applicable.	Not applicable.
Technical Competency 17: Apply a management system and develop an information security management plan	Identify and follow organisational policies and security management processes for information and cyber security. Operate according to service level agreements or employer defined performance targets. Develop an information security management plan for a defined business area/activity in accordance with ISO27001 or similar.	Not applicable.	Not applicable.

Technical Competency 18: Configure and use security technology components and key management.	Select and configure at least 2 types of common security hardware and software components to implement a given security policy. Design a system employing a crypto to meet defined security objectives. Develop and implement a key management plan for the given scenario/system.	Not applicable.	Not applicable.
Technical Competency 19: Design and evaluate a system to a security case	Design and build a simple system in accordance with a simple security case. Provide evidence that the system has properly implemented the security controls required by the security case. The system could be either at the enterprise, network or application layer.	Ensure the system encompasses two out of enterprise, network or application layers.	Ensure the system encompasses all three out of enterprise, network and application layers.
Technical Competency 20: Architect, analyse and justify a secure system	Apply interpretation of security policy and risk profiles to design secure architectural solutions that meet security objectives, mitigate the risks and conform to legislation in a representative business scenario. Critically analyse secure architectural solutions and security controls against defined security objectives to assess how effectively risks are mitigated, legal requirements and business requirements are met. Identify and describe the means by which the risk owner can have confidence that the solution mitigates the risks to an acceptable level.	Propose, with reasoned justifications, additional security controls to mitigate identified weaknesses.	Propose additional means by which the risk owner can have confidence that the solution mitigates the risks to an acceptable level and relate the proposed measures to a publicly available definition or standard of cyber security assurance.
Technical Competency 21: Develop and assurance strategy	Develop an assurance strategy for a defined system, selecting appropriate assurance approaches.	Not applicable.	Not applicable.

Technical Competency 22: Security monitoring, analysis and intrusion detection. Recognise anomalies & behaviours	Recognise anomalies in observed network data structures (including. by inspection of network packet data structures) and network 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. Integrate and correlate information from various sources (including log files from different sources, network 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 network security breach. Characterise an anomaly in terms of its potential impact on the organisation.	Not applicable.	Not applicable.
Technical Competency 23: Manage intrusion response, including with 3rd parties.	Manage local response to non-major incidents in accordance with a defined procedure. Interact and communicate effectively with the incident response team/process and/or customer or other external incident response team/process for incidents.	Not applicable.	Not applicable.
Technical Competency 25: Organise testing & investigation work in accordance with legal and ethical requirements	Organise cyber security testing work within a legal and ethical framework (under English jurisdiction). Organise cyber security incident investigation work within a legal and ethical framework (under English jurisdiction). Secure evidence appropriately to support legal proceedings.	Not applicable.	Not applicable.

Technical Competency 26: Develop & apply information security policy to implement legal or regulatory requirements.	Develop an information security policy or process to address an identified risk. Develop an information security policy within a defined scope to take account of a minimum of one law or regulation relevant to cyber security.	Not applicable.	Not applicable.

Technical Knowledge and Understanding tested

The standard	Minimum for a pass. The apprentice can…	Merit: in addition to the pass requirement, the apprentice can demonstrate an understanding of…	Distinction: in addition to the pass and merit requirements, the apprentice can demonstrate an understanding of…
Technical Knowledge and Understanding 2: Network foundations, connections, internetworking, protocols, standards performance, security and server virtualisation.	Describe the fundamental building blocks (e.g. routers, switches, hubs, storage, transmission) and typical architectures (e.g. server/client, hub/spoke) of computers networks and the Internet. Explain what is meant by data and protocol and how they relate to each other. Describe an example data format and a simple protocol in current use (using protocol diagrams). Describe example failure modes in protocols, for example reasons why a protocol may 'hang' and the effect on a protocol of data communication errors, Describe at least one approach to error control in a network. Describe the main features of network protocols in widespread use on the Internet and their purpose and relationship to each other, including the physical and data link layer. *(e.g. https, HTTP, SMTP, SNMP, TCP, IP, BGP, DNS etc).*	How to configure and optimise components in a computer network to meet a given requirement.	How to troubleshoot complex problems in network designs and implementations.

	Explain some of main factors that affect network performance (e.g. the relationship between bandwidth, number of users, nature of traffic, contention) and propose ways to improve performance (e.g. application of traffic shaping, changes to architecture to avoid bottlenecks, network policy that prohibit streaming protocols). Understand the impact of the employment of virtualisation techniques to networks and its role in 'Cloud'. Understand network-based attacks: eavesdropping / sniffing, man-in-the-middle, spoofing, session hijacking, denial of service, traffic redirection, routing attacks, traffic analysis, malware. Understand network monitoring and mapping. Discuss issues that may arise in the day to day operation of networks. Describe the main routing protocols in current use in computer networks and explain the differences between static and dynamic routing protocols and the pros and cons of each in different circumstances.		
Technical Knowledge and Understanding 3: Information management, big data concepts, statistical techniques, database concepts and data quality.	Understand: • Benefits and limitations of 'big data' approaches • Components and architectures employed in systems for big data (e.g. Hadoop cluster) • Tools and techniques for analysing large heterogeneous data sets • Graph theory Understand information management concepts:	Not applicable.	Not applicable.

	• information storage and retrieval; • information capture and representation; • searching, retrieving, linking, navigating. Understand database concepts: • components of database systems; • design of core DBMS functions (e.g. query mechanisms, access methods); • database architecture and query language.		
Technical Knowledge and Understanding 4: Computer architecture, digital logic, machine level representation of data.	Understand: • classical computer architectures; • virtualised architectures; • digital logic, static and dynamic digital systems; • machine level representation of data; • assembly level machine organisation; • memory system organisation and architecture; • interfacing and communication.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 5: Operating System (OS), principles, architectures, features, mechanisms, security features and exploits.	Understand that an OS defines an abstraction of hardware and manages resource sharing among a computer's users: • OS principles; • concurrency and synchronisation; • scheduling and dispatch; • memory management; • security and protection; • kernel security and protection; • file systems; • I/O system. Understand typical OS security features and how these may themselves be exploited.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 6: Algorithm	Understand: • algorithms and program design; • fundamental programming concepts;	Not applicable.	Not applicable.

and programme design, concepts, compilers and logic. Programming languages.	• fundamental data structures; • typical program development environment and methods. Understand that programming languages are the medium through which programmers precisely define concepts, formulate algorithms, and reason about solutions: • object-oriented programming; • functional programming; • event driven and reactive programming; • language translation and execution; • syntax analysis; • compiler semantic analysis; • code generation; • coding in assembler; • machine code;scripting language. •		
Technical Knowledge and Understanding 7: Algorithms, complexity and discrete maths.	Understand the central concepts of algorithms and complexity: • analysis; • algorithmic strategies; • fundamental data structures and strategies; • automata, computability and complexity. Understand the foundations of discrete mathematics applied to computing: • sets, relations and functions; • logic and proof techniques; • graphs and trees.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 8: How software interacts with the hardware and real-world	Understand how software can interact with the hardware/physical environment: • how software running on a microprocessor may interact with signals from sensors or effect actuators;	Not applicable.	Not applicable.

environment and security issues.	• identify how a threat actor may exploit the external environment or software/hardware interface and mitigations that may be employed. Understand the specific security challenges posed by 'embedded systems' (i.e. with size, power, processor, memory, scale, bandwidth limitations) for example 'Internet of Things' (IoT) devices.		
Technical Knowledge and Understanding 9: Malware, reverse engineering, obfuscation.	Understand the low-level mechanisms used by current malware: • machine level instruction set; • reverse engineering techniques; • reverse engineering for malware analysis; • de-obfuscation of obfuscated code; • anti-debugging mechanisms	Understand how to overcome the protection mechanisms used by malware.	How to script / compose custom tool sets for the analysis of more complex malware.
Technical Knowledge and Understanding 10: Defensive programming, malware resistance, code analysis, formal methods, good practice.	Knowledge and understanding of defensive programming (input validation, least privilege, defence in depth, data sanitization, etc.) Understanding of how to resist malware techniques (memory corruption, code injection, user/kernel space vulnerabilities, privilege escalation, etc.) Use of design patterns for developing secure software. Understand how to use compiler features to support creation of secure code. Understand how to apply static and dynamic code analysis techniques. Obtain and apply sources of secure programming practices, including employer or software development organisation, for different types of software systems (OWASP, CERT, etc.).	The types and range of vulnerabilities in software.	Approaches to the mitigation of vulnerabilities.

	Describe at least 1 formal method (e.g. CSP) that may be applied to software development and its strengths and weaknesses when applied to development of software with security properties. Defensive programming		
Technical Knowledge and Understanding 11: System development principles, tools, approaches, complexity, software engineering	Understand of how the different aspects in a software development lifecycle combine to deliver a successful outcome. (Considering: meeting a need, design, trade-offs, implementation, deployment, support, evolution, validation, verification and assurance). Describe different approaches to developing software, including sequential, iterative/agile approaches. Give an explanation of the advantages and disadvantages of different software development processes, and justify choice of process in different contexts. Understand how to select and use different tools and environments that support software development at different stages in the lifecycle. Understand the principles of systems engineering, including all aspects of technology, people, culture and process and the environment within which a system of interest exists and operates. Explain the benefits of a system approach to dealing with challenges arising from complexity, emergence, adaption and co-evolution.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 12: Threats, vulnerabilities, impacts and	Explain how cyber security concepts apply to ICT infrastructure.	How to research, analyse and evaluate security threats and hazards to a specified system including technology and considering services and processes.	How to devise mitigations to defend against security threats and hazards to a specified system including technology and considering services and processes.

mitigations in ICT systems and the enterprise environment	Describe the fundamental building blocks and typical architectures and identify some common vulnerabilities in networks and systems. Understand vulnerabilities in computer networks and systems (for example un-secure coding and unprotected networks) and how they can be exploited. Understand the impact of identified vulnerabilities in the organisation's context. Understand the human dimension of cyber security the need to adopt an adversarial thinking approach to system development and analysis. Analyse how an employee may enable a successful attack chain without realising it. Describe some things that may increase or decrease risks related to an organisation's 'cyber culture'. Identify the vulnerabilities in organisations security management system. Identify the links between physical, logical, personal and procedural security. Describe ways to defend against cyber-attack techniques. Describe the existing threat landscape. Understand how to apply relevant techniques for horizon scanning, including use of recognised sources of threat intelligence, to keep the view of the threat landscape up to date. Describe threat trends and the significance of identified trends. Understand the threat intelligence lifecycle and the concepts of threat actors and attribution. Evaluate and describe the significance, value and limitations of a given threat analysis.		

Technical Knowledge and Understanding 14: structured and ethical intelligence analysis, methods, techniques	Know how to create a reasoned argument employing evidence to support a position. Know how typical threat actors' actions appear in typical sources of information. Know how to source intelligence ethically so that it may be used as required. Understand methods an attacker/threat actor may use to build knowledge of a system they have limited or no direct access to: • phishing; • exploiting an insider; • port scanning; • open source intelligence.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 15: Management of cyber security risk, tools and techniques	Understand: • asset valuation and management concepts; • risk analysis methodologies in common use; • risk appetite and risk tolerance concepts; • economics of security concepts; • different ways of treating risk (mitigate, transfer, accept etc.); • principles of system risk modelling; • a system risk modelling methodology. Show awareness of at least 1 widely used enterprise modelling technique, e.g. employing UML.	How to employ one of the following methods to inform risk analysys: SABSA, DBSy, CVVS scoring, STRIDE or NIST 800-154.	How to ensure that, in comparing and contrasting techniques, options are identified for investment in measures to mitigate cyber risk based on analysis and modelling in an enterprise scenario.
Technical Knowledge and Understanding 16: Quantitative and qualitative risk management theory and practice, role of risk stakeholders.	Understand risk assessment and risk management methodologies and different approaches to risk treatment (mitigate, transfer, accept, etc.) and risk management in practice with examples (which may be technical, business process, or other).	Not applicable.	Not applicable.

	Understand that risks may be described in qualitative, quantitative terms or some combination thereof. Understand the role of the risk owner and contrast that role with other stakeholders.		
Technical Knowledge and Understanding 17: Concepts and benefits of security management systems, governance and international standards.	Explain the key concepts and benefits of applying an information security management system by reference to an internationally recognised standard (ISO27001, or similar). Explain the need for appropriate governance, organisational structure, roles, policies, standards and guidelines for cyber and information security, and how they work together to deliver identified security outcomes. Explain how an organisation's security policies, standards and governance are supported by provisioning and access rights (e.g. how identity and access management are implemented and maintained for a database, application or physical access control system). Describe how cyber security policies and procedures are used in different organisational environments and affect individuals and organisations. Understand the roles of experts in the cyber security industry, how they are recognised, and the work they do. Understand how to effectively use organisations such as a CERT, OSINT provider and incident response provider.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 18: Security	Describe common types of security hardware and software which are used to protect systems (e.g. firewalls, encryption for data at rest, encryption for		

components: how they are used for security / business benefit. Crypto and key management.	communication, intrusion detection systems (IDS), intrusion protection systems (IPS), identity and access management (IDAM) tools, anti-virus (AV), web proxy, application firewalls, cross domain components, hardware security module (HSM), TPM, UTM) and explain how each may be used to deliver risk mitigation or implement a security case, understanding the benefits/limitations, and taking into account the implicit assurance (including supplier assurance and considering the benefits and risks of open source options) of the component, describing any residual risks. Describe the main cryptographic techniques (e.g. symmetric, public key, secure hash, digital signing, block cipher etc.), how they are applied and to what end and their limitations (including study of some examples of badly applied or implemented cryptographic techniques). Explain the significance of key management and the main features, benefits and limitations of symmetric and public key cryptosystems and the significance of entropy. Describe the role of cryptographic techniques in a range of different systems (e.g. GSM, Chip&PIN, common hard disk encryption, TLS, SSL, privacy enforcing technology) and the practical issues introducing such into service and updating them.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 19: How to compose a justified security case	Compose a security case, deriving objectives with reasoned justification in a representative business scenario.	How to encompass two out of enterprise, network or application layers in the design of a system.	How to encompass all three out of enterprise, network and application layers in the design of a system.
Technical Knowledge and Understanding 20: Understand security assurance, how to	Understand how to interpret security policy and risk profiles into secure architectural solutions that meet security objectives, mitigate the risks and	How to make reasoned justifications for additional security controls to mitigate identified risks.	How to make a clearly argued case for additional security measures in which the risk owner and have confidence that

achieve it and how to apply security principles.	conform to legislation in a representative business scenario. Describe the fundamental security technology building blocks and typical architectures and architecture frameworks. Understand design principles for architecting a secure system (separation of concerns, fail-safe/fail-secure, defence in depth, least privilege, how to apply proven security architectural patterns from reputable sources, how to incorporate appropriate security controls). Understand security assurance ('trustworthy' versus 'trusted') and how an architecture may be assured.		the solution mitigates the risk to an acceptable level.
Technical Knowledge and Understanding 21: Assurance concepts and approaches.	Explain the difference between 'trusted' and 'trustworthy' and explain what assurance is for in security. Describe the main approaches to assurance (intrinsic, extrinsic, design & implementation, operational policy & process) and give examples of how these might be applied at different stages in the lifecycle of a system. Describe at least one current system of extrinsic assurance (e.g. red teaming, security testing, supply chain assurance, Common Criteria) explaining the benefits and limitations. Explain what 3rd party testing (e.g. 'ethical hacking') is and how it contributes to assurance. Describe at least 2 ways an organisation can provide intrinsic assurance.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 22: How to	Understand network monitoring and logging techniques and technologies.	Not applicable.	Not applicable.

diagnose cause from observables. Application of SIEM (Security Information and Event Management) tools and techniques.	Understand how attack techniques and vulnerabilities manifest in network monitoring and logging systems so that (for example) analysis of a network log or the output of a network monitoring tool may reveal the likely means of an attack. Understand the relative merits of manual and automated techniques. Understand the relative merits of signature based anomaly detection and algorithmic anomaly detection. Understand how statistical techniques might be applied in support of analysis of cyber security incidents.		
Technical Knowledge and Understanding 23: Cyber incident response, management, escalation, investigation and third-party involvement.	Understand and advises others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation. Understand how to communicate effectively with the incident response team/process and/or customer or other external authority incident response team/process for incidents.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 25: Applicability of laws, regulations and ethical standards.	Understand applicability of laws and regulations to security testing of 3rd parties ('ethical hacking', 'pen-testing'). Describe by reference to at least 1 generally recognised and relevant professional body the ethical responsibilities of a cyber-security professional. Understand applicability of laws and regulation to intelligence collection and analysis, and the relationship to data protection, human rights and privacy.	Not applicable.	Not applicable.
Technical Knowledge and Understanding 26: Legal	Describe the legal responsibilities of system users and how these are communicated effectively.	Not applicable.	Not applicable.

responsibilities of system owners, users, employers, employees.	Understand laws and regulations applicable to cyber security, personal and sensitive data, employee protection and monitoring, relevant to England and one other non- UK jurisdiction. This understanding should encompass what is prohibited (i.e. an offence), protections, legal risks and obligations.		

Underpinning professional, interpersonal and business skills tested

The standard	Minimum for a pass. The apprentice can…
Fluent in written communications and able to articulate complex issues.	Produce well-structured and concise written work that sets out complex technical matters in ways which that would be accessible to non-technical recipients as well as technical staff (as appropriate).
Analytical and critical thinking skills for Technology Solutions development and can systematically analyse and apply structured problem-solving techniques to complex systems and situations.	Evaluate information and then make a rational decision on the approach to take to solve the problem, based on their findings; spot trends in data and articulate the implications.
Can conduct effective research, using literature and other media.	Put into practice sound research techniques (using literature and other media) and articulate in writing and/or verbally how they have utilised the findings in their work.
Logical thinking and creative approach to problem solving.	Observe and analyse phenomena, reactions and feedback, and draw logical conclusions based on that input.
Able to demonstrate a 'security mind-set' (how to break as well as make).	Think about how things can be made to fail, as well as about how things can be made to work.

Behaviours tested

Behaviours	Minimum for a pass. The apprentice can…

Demonstrates business disciplines, ethics and courtesies, demonstrating timeliness and focus when faced with distractions and the ability to complete tasks to a deadline with high quality	Act in a professional way as required in the cyber security context.
Flexible attitude and ability to perform under pressure.	Deliver the best project outcomes against goals, re-prioritising as necessary, even in challenging circumstances.

ANNEX 2. TECHNCIAL DISCUSSION (Fail / Pass only)

NOTE: the Technical Discussion is informed by the outputs contained in the portfolio the apprentice must have submitted before the Technical Discussion takes place.

An apprentice will fail the Technical Discussion if he/she has not met all of the pass criteria below.

Technical Competencies tested

The standard	Minimum for a pass. The apprentice can…
Technical Competency 13: Assess culture & individual responsibilities	Assess security culture using a recognised approach. Design and implement a simple security awareness campaign to address a specific aspect of security culture. Demonstrate good personal security hygiene appropriate to the employer context.
Technical Competency 20: Architect, analyse and justify a secure system	Identify and describe the means by which the risk owner can have confidence that the solution mitigates the risks to an acceptable level.
Technical Competency 21: Develop an assurance strategy	Develop an assurance strategy for a defined system, selecting appropriate assurance approaches.

Technical Knowledge and Understanding tested

The standard	Minimum for a pass. The apprentice can…
Technical Knowledge and Understanding 1: foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance	Understand why cyber security matters – the importance to business and society, including consideration of the significance of cyber security to critical and safety critical systems (including healthcare systems, critical national infrastructure, industrial plant automation, autonomous vehicles, mass transportation, internet of things). Understand concepts: security, identity, confidentiality, integrity, availability, threat, vulnerability, impact, consequences risk and hazard. Also how these relate to each other and lead to risk and harm. Describe attack techniques and sources of threat and the role of human behaviour. Explain how attack techniques combine with motive and opportunity to become a threat. Understand the concept of an attack chain: how to put an attack into a larger (greater than one's own organisation) context, or as part of a more sophisticated attack. Understand security assurance concepts (can explain what assurance is for in security, and 'trustworthy' versus 'trusted') and how assurance may be achieved in practice (can explain what penetration testing is and how it contributes to assurance; and extrinsic assurance methods).
Technical Knowledge and Understanding 13: Human dimensions of cyber security	Understand the role of information security awareness and training and is aware of the benefits of behavioural analysis and security culture management in maintaining good information security. Understand the motivations and ways of thinking of different classes of threat actors, criminal intent, activism, state actors, hackers, and how this drives the behaviour of the threat actors in order to understand how to tailor mitigations for the different classes of threat actor. Understand the Insider threat and the difference between malicious intent and human error. Understand the need for 'usable security' in which security mechanisms are designed to take into account the ways in which people work – i.e., the mechanisms are not too time consuming to use or so complex that people make mistakes or try to by-pass them. Understand how social engineering and phishing exploit human behaviour as means of attack.
Technical Knowledge and Understanding 20: Understand security assurance, how to achieve it and how to apply security principles	Understand design principles for architecting a secure system (separation of concerns, fail-safe/fail-secure, defence in depth, least privilege, how to apply proven security architectural patterns from reputable sources, how to incorporate appropriate security controls).

Technical Knowledge and Understanding 21: Assurance concepts and approaches.	Explain the difference between 'trusted' and 'trustworthy' and explain what assurance is for in security. Describe the main approaches to assurance (intrinsic, extrinsic, design & implementation, operational policy & process) and give examples of how these might be applied at different stages in the lifecycle of a system. Describe at least one current system of extrinsic assurance (e.g. red teaming, security testing, supply chain assurance, Common Criteria) explaining the benefits and limitations. Explain what 3rd party testing (e.g. 'ethical hacking') is and how it contributes to assurance. Describe at least 2 ways an organisation can provide intrinsic assurance.
Technical Knowledge and Understanding 24: Legal, regulatory, compliance and standards environment.	Describe the key features of the main laws applicable to England that are relevant to cyber security issues (including legal requirements that affect individuals and organisations), e.g.: Computer Misuse Act, Data Protection Act, GDPR, Human Rights Act. Describe the cyber security standards and regulations and their consequences for at least 2 sectors (e.g. Government, finance, telecommunications, petrochemical/process control), comparing and contrasting the differences. Describe the implications of international laws and regulations that affect organisations, systems and users in the UK, movement of data and equipment across international borders and between jurisdictions (e.g. Digital Millennium Act, ITAR, Safe Harbour). Describe the legal issues relevant to cryptography (UK, EU and US export control of cryptography and the Wassenaar Arrangement). Explain the benefits & costs and the main motives for uptake of significant security standards such as Common Criteria, PCI-DSS, FIPS-140-2, Government (e.g. UK NCSC) schemes.

Underpinning professional, interpersonal and business skills tested

The standard	Minimum for a pass. The apprentice can…
Makes concise, engaging and well-structures verbal presentations, arguments and explanations.	Give well-structured verbal presentations, arguments and explanations that take into account the audience's needs and are convincing and persuasive.
Able to deal with different, competing interests within and outside the organisation with excellent negotiation skills.	Understand competing interests and articulate (in writing or verbally) how they weigh these up, reach conclusions on the best way forward, and how they seek to persuade others to adopt the approach they have decided on.

Able to identify the preferences, motivations, strengths and limitations of other people and apply these insights to work more effectively with and to motivate others.	Articulate effectively their approach to working with and motivating others.
Able to work effectively with others to achieve a common goal.	Articulate effectively how they: - Encourage and facilitate cooperation and trust - Foster team spirit, commitment, and group identity - Work with others to achieve shared goals
Competent in active listening and in leading, influencing and persuading others.	Articulate effectively how they listen and try to understand different perspectives and how they approach influencing and persuading others.
Able to give and receive feedback constructively and incorporate it into his/her own development and life-long learning.	Describe how they handle feedback (eg without getting defensive) and their approach to offering constructive feedback (and how they have learnt from it).
Able to put forward, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business need, using open questions and summarising skills and basic negotiating skills.	Articulate effectively how they have achieved the statement on the standard in a real-world work environment.

Behaviours tested

Behaviours	**Minimum for a pass. The apprentice can…**
A thorough approach to work in the cyber security role	Show a commitment to delivering the best outcomes they are capable of.