

**MODULE SPECIFICATION**

|  |
| --- |
| **Part 1: Information** |
| **Module Title** | End point assessment (EPA) |
| **Module Code** | CY402 | **Level** | 6 (UWE 3) |
| **For implementation from** | September 2020  |
| **UWE Credit Rating** | 10 | **ECTS Credit Rating** | 5 |
| **Faculty** | Environment and Technology | **Field** |  |
| **Department** | Computer Science and Creative Technologies |
| **Contributes towards**  | BSc (Hons) Cyber Security Technical Professional Compulsory |
| **Module type:**  | Standard  |
| **Pre-requisites**  | Completion of all prior modules (350 credits) |
| **Excluded Combinations**  | None  |
| **Co- requisites**  | None  |
| **Module Entry requirements** | None |
|  |
| **Part 2: Description**  |
| 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 EPA starts after the Gateway has been passed. 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 (KSBs) requirements set out in the occupational standard; and
2. the apprentice has completed and passed all the modules in years 1-3 (350 credits)
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

**Portfolio requirements** 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. Employers, with support from the institution, will assist the apprentice to assemble their portfolio. The KSBs that are covered by the portfolio are those in the apprenticeship standard. 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
* a brief introduction/commentary by the apprentice, produced towards the end of their apprenticeship and highlighting, where appropriate, anything they would do differently
* evidence from between six and eight real work projects/pieces of work;
* a testimonial from the employer, relating to the behaviour shown in table 4
* written feedback from peers, colleagues and stakeholders
* demonstration of the business impact achieved during the apprenticeship
* evidence of teamworking; and
* a signed statement from the employer and the institution confirming this as being the apprentice’s own work and confirming that, in their view, the work demonstrates the required KSBs
* a signed statement from the apprentice confirming this as their own work.

The portfolio presents evidence from real-work projects and is used to help the apprentice answer questions in the Technical Discussion. The apprentice must provide the portfolio to the end point assessment institution at least one week before the commencement of the Technical Discussion point assessment. The portfolio will be developed over a period of 6 months and must include evidence from between six and eight real work projects/pieces of work. Evidence can be in the form of:* 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

 Evidence of the technical competencies to be submitted in the EPA portfolio are:* Design, build, configure, optimise, test and troubleshoot simple and complex networks.
* Apply statistical techniques to large data sets. Identify vulnerabilities in big data architectures and deployment.
* Build test and debug a digital system to a specification.
* Configure an Operating System in accordance with security policy. Identify threats and features.
* Write, test, debug programs in high and low level languages and scripts.
* Design, implement and analyse algorithms.
* Construct software to interact with the real world and analyse for security exploits.
* Analyse malware & identify its mechanisms.
* Apply secure programming principles and design patterns to address security issues.
* Apply system engineering and software development methodologies and models.
* Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations.
* Assess culture & individual responsibilities.
* Undertake ethical system reconnaissance and intelligence analysis.
* Undertake risk modelling, analysis and trades.
* Undertake risk assessment to an external standard.
* Apply a management system and develop an information security management plan.
* Configure and use security technology components and key management.
* Design & evaluate a system to a security case.
* Architect, analyse & justify a secure system.
* Develop an assurance strategy.
* Security monitoring, analysis and intrusion detection. Recognise anomalies & behaviours.
* Manage intrusion response, including with 3rd parties.
* Organise testing & investigation work in accordance with legal & ethical requirements.
* Develop & apply information security policy to implement legal or regulatory requirements.

**Technical Discussion**In the technical discussion the apprentice will cover these technical knowledge, competencies and behaviours:* Assess culture & individual responsibilities.
* Architect, analyse & justify a secure system.
* Develop an assurance strategy.
* Foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance.
* Human dimensions of cyber security.
* Understand security assurance, how to achieve it and how to apply security principles.
* Assurance concepts & approaches.
* Legal, regulatory, compliance & standards environment.

Behaviours* Makes concise, engaging and well-structured verbal presentations, arguments and explanations.
* Able to deal with different, competing interests within and outside the organization with excellent negotiation skills.
* 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.
* Able to work effectively with others to achieve a common goal.
* Competent in active listening and in leading, influencing and persuading others.
* Able to give and receive feedback constructively and incorporate it into his/her own development and life- long learning.
* 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.
* A thorough approach to work in the cyber security role.
 |
| **Part 3: Assessment**  |
| 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; (Component A) and(b) A Technical Discussion (Component B) 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).  |
|  |
| Identify final timetabled piece of assessment (component and element) | B1 |
| **% weighting between components A and B** (Standard modules only) | **A:**  | **B**:  |
| **50** | **50** |
|  |
| **First Sit** |
| **Component A** (controlled conditions)**Description of each element** | **Element weighting** |
| 1. Practical Test (48 hours +-10%) within a 2-week period
 | 100 |
| **Component B** **Description of each element** | **Element weighting** |
| 1. Technical Discussion (120 minutes +/- 10%)
 | 100 |
| **Resit (further attendance at taught classes is not required)** |
| **Component A** (controlled conditions)**Description of each element** | **Element weighting** |
| 1. Practical Test (48 hours +-10%) within a 2 week period | 100 |
| **Component B Description of each element** | **Element weighting** |
| 1. Technical Discussion (120 minutes +/- 10%) | 100 |
|  |
| **Part 4: Learning Outcomes & KIS Data** |
| **Learning Outcomes** | On successful completion of this module students will be graded:FAIL – one or more of the KSBs tested have not met the Pass criteriaPASS – all the KSBs have met the Pass criteriaMERIT - 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 *See the module handbook for details of the Technical Competencies and Technical Knowledge*  |
| **Key Information Sets Information (KIS)****Contact Hours****Total Assessment** |  The table below indicates as a percentage the total assessment of the module which constitutes a;**Technical discussion****Practical exam**  |
| **Reading List** | There is no required or recommended reading for this module |

***FOR OFFICE USE ONLY***

|  |  |
| --- | --- |
| **First Approval Date (and panel type)** | *Date of first {panel} approval*  |
| **Revision ASQC Approval Date** *Update this row each time a change goes to ASQC* |  | **Version**  | *1* | *Link to RIA*  |
|  |  |  |
|  |  |  |
|  |  |  |