

**MODULE SPECIFICATION**

|  |
| --- |
| **Part 1: Information** |
| **Module Title** | Security assurance and security case development |
| **Module Code** | CY301 | **Level** | 6  |
| **For implementation from** | September 2020  |
| **UWE Credit Rating** | 30 | **ECTS Credit Rating** | 15 |
| **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**  | None |
| **Excluded Combinations**  | None  |
| **Co- requisites**  | None  |
| **Module Entry requirements** | None |
|  |
| **Part 2: Description**  |
| There are recognised IT security design principles which can be applied to IT systems and software. These include security architectures that incorporate hardware and software components. A security case should take these principles and architectures into account and include:* A clear definition of the security objectives of the case
* Threats that are likely to exist against the target system (physical, intrusion, malware)
* Risks to the system, measured in probabilities (very likely, likely and unlikely)
* Potential impact / severity (major, moderate, minor)
* Strategies for dealing with risks (avoid, accept, mitigate, transfer)

Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.This module will be based on ensuring that apprentice’s practical skills and knowledge gained in the block release sessions are carried into the workplace to inform their employment and generation of evidence of competency. You will cover:* composing a security case, deriving objectives with reasoned justification in a representative business scenario
* interpreting security policy and risk profiles into secure architectural solutions that meet security objectives, mitigate the risks and conform to legislation in a representative business scenario
* fundamental security technology building blocks and typical architectures and architecture frameworks
* design principles for architecting a secure system, for example
	+ separation of concerns, fail-safe/fail-secure, defence in depth, least privilege
	+ application of proven security architectural patterns from reputable sources
	+ incorporation of appropriate security controls
* security assurance and how an architecture may be assured
* security assurance:
	+ role in cyber security
	+ ‘trustworthy’ versus ‘trusted’
	+ assurance of an architecture
* approaches to assurance
	+ intrinsic, extrinsic, design and implementation, operational policy and process
	+ examples of how these might be applied at different stages in the lifecycle of a system.
* at least one current system of extrinsic assurance
	+ e.g., red teaming (penetration testing), security testing, supply chain assurance, Common Criteria
	+ benefits and limitations
* third party testing (e.g., ethical hacking) and how it contributes to assurance
* at least 2 ways an organisation can provide intrinsic assurance
 |
| **Part 3: Assessment**  |
| **Assessment 1 – Component A** A written, unseen, 2-hour exam will test the apprentice’s understanding of security assurance and architecting a secure system. **Assessment 2 – Component B** Apprentices will develop and report on a security case, based on a given, or real (from their workplace) scenario. The work will be recorded in a workbook, along with a reflection.  |
|  |
| 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****(as % of component)** |
| 1. Exam (2 hours) | 100% |
| **Component B** **Description of each element** | **Element weighting****(as % of component)** |
| 1. Workbook | 100% |
| **Resit (further attendance at taught classes is not required)** |
| **Component A** (controlled conditions)**Description of each element** | **Element weighting(as % of component)** |
| 1. Exam (2 hours) | 100% |
| **Component B Description of each element** | **Element weighting(as % of component)** |
| 1. Workbook | 100% |
|  |
| **Part 4: Learning Outcomes & KIS Data** |
| **Learning Outcomes** | On successful completion of this module students will be able to:Understand security assurance, how to achieve it and how to apply security principles (component A)Understand the design principles for architecting a secure system (component A) Develop a security case for a real organisation, using recognised methods and to an internationally recognised standard (component B) Reflect on the process of developing a security case, justifying methods used and /or proposing alternatives (component B)  |
| **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;**Written Exam**: Unseen or open book written exam**Coursework**: Written assignment or essay, report, dissertation, portfolio, project or in class test **Practical Exam**: Oral Assessment and/or presentation, practical skills assessment, practical exam (i.e. an exam determining mastery of a technique)  |
| **Reading List** | Reading list to be added  |

***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*  |
|  |  |  |
|  |  |  |
|  |  |  |