

**MODULE SPECIFICATION**

|  |
| --- |
| **Part 1: Information** |
| **Module Title** | Risk and information management |
| **Module Code** | CY302 | **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**  |
| Risk assessments are used to identify, estimate, and prioritize risk to organisational operations (i.e., mission, functions, image, finance and reputation), organisational assets, individuals and other organisations, resulting from the operation and use of information systems.In order to assess risk, the systems need to be explored for weaknesses, either technical or social. Reconnaissance methods emulate those of attackers.This module examines: * the methods and roles of those involved in attacking systems
* analysing system weaknesses
* assessing the associated risks and managing them

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:* the role of information security awareness and training
* behavioural analysis and security culture management in maintaining good information security
* 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
* tailoring mitigations for the different classes of threat actor
* social engineering and phishing
* insider threat
	+ malicious intent and human error
* usable security
* creation of a reasoned argument employing evidence to support a position
* how threat actors’ actions appear in typical sources of information
* sourcing intelligence ethically so that it may be used as required
* methods attackers/threat actors may use to build knowledge of a system they have limited or no direct access to, such as:
	+ phishing
	+ exploiting an insider
	+ port scanning
* open source intelligence
* 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
* an enterprise modelling technique such as UML
* risk assessment and risk management methodologies
* approaches to risk treatment (mitigate, transfer, accept, etc.)
* risk management in practice
	+ examples such as technical, business process, or other
* description of risk in qualitative, quantitative, or mixed terms
* role of risk owner, contrasting role with other stakeholders
 |
| **Part 3: Assessment**  |
| **Assessment 1 – Component A** Apprentices will write a report (1,500 words) on their research into the roles and actions people play in cybersecurity, both beneficial and harmful. **Assessment 2 – Component B** Apprentices will be provided with a case study of a system (in document and physical form) for them to perform a complete risk assessment. They will submit a notebook of their findings and methods, alongside a formal documented assessment.  |
|  |
| Identify final timetabled piece of assessment (component and element) | B1 |
| **% weighting between components A and B** (Standard modules only) | **A:**  | **B**:  |
| **40%** | **60%** |
|  |
| **First Sit** |
| **Component A** **Description of each element** | **Element weighting****(as % of component)** |
| 1. A report (1,500) words | 100% |
| **Component B** **Description of each element** | **Element weighting****(as % of component)** |
| 1. Notebook and formal risk assessment | 100% |
| **Resit (further attendance at taught classes is not required)** |
| **Component A** **Description of each element** | **Element weighting(as % of component)** |
| 1. A report (1,500) words | 100% |
| **Component B Description of each element** | **Element weighting(as % of component)** |
| 1. Notebook and formal risk assessment | 100% |
|  |
| **Part 4: Learning Outcomes & KIS Data** |
| **Learning Outcomes** | On successful completion of this module students will be able to:Explain the human dimensions of cybersecurity (component A)Apply structured and ethical intelligence analysis, methods, techniques (component A)Undertake risk modelling, analysis and trades (component B)Undertake risk assessment to an external standard (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*  |
|  |  |  |
|  |  |  |
|  |  |  |