

**MODULE SPECIFICATION**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Part 1: Information** | | | | | | | | |
| **Module Title** | | Cybersecurity incident management and professionalism | | | | | | |
| **Module Code** | | CY303 | | **Level** | | 6 | | |
| **For implementation from** | | September 2020 | | | | | | |
| **UWE Credit Rating** | | 20 | | **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** | | | | | | | | |
| Managing security incidents requires a rigorous approach and may have to be performed in real time. There are defined processes with key stages:   * Writing a plan * Training * Defining roles and responsibilities * Establishing and testing a data recovery plan * Identifying potential security incidents through monitoring and report all incidents. * Assessing identified incidents to determine the appropriate next steps for mitigating the risk. * Responding to the incident by containing, investigating, and resolving it * Complying with legal and regulatory requirements * Learning and documenting lessons   Apprentices will be instructed and practice incident management. As part of this modules they will also research and investigate the legal, ethical and regulatory requirements.  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:   * network monitoring and logging techniques and technologies * how attack techniques and vulnerabilities manifest in network monitoring and logging systems   + e.g., analysis of a network log or the output of a network monitoring tool may reveal the likely means of an attack * the relative merits of manual and automated techniques * the relative merits of signature-based anomaly detection and algorithmic anomaly detection * how statistical techniques might be applied in support of analysis of cyber security incidents * integration and correlation of information from various sources * cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation * how to communicate with incident response team/process and/or customer or other external authority incident response team/process for incidents * 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. * the cyber security standards and regulations and their consequences for at least 2 sectors, e.g.:   + government, finance, telecommunications, petrochemical/process control   + compare and contrast the differences * 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 * legal issues relevant to cryptography, e.g.:   + UK, EU and US export control of cryptography, the Wassenaar Arrangement * benefits and 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. * applicability of laws and regulations to security testing of 3rd parties (‘ethical hacking’, ‘pen testing’) * ethical responsibilities of a cyber security professional * applicability of laws and regulation to intelligence collection and analysis, and the relationship to data protection, human rights and privacy * the legal responsibilities of system users and how these are communicated effectively * laws and regulations applicable to cyber security, personal and sensitive data, employee protection and monitoring, relevant to England and one other non- UK jurisdiction   + should encompass what is prohibited (i.e., an offence), protections, legal risks and obligations * social context * analytical tools * professional ethics * intellectual property * privacy * professional communication * sustainability | | | | | | | | |
| **Part 3: Assessment** | | | | | | | | |
| **Assessment 1 – Component A**  During the college sessions the apprentices will complete a series of tasks in a workbook. They will commence with detecting and analysing a security incident. They will then have to demonstrate how the incident is managed.  **Assessment 2 – Component B**  Apprentices will write a report (1,500 words) detailing how the security policies in place, or that they have written, in their workplace, implement the required legal and regulatory requirements. They should identify any actions required to remedy any oversights. | | | | | | | | |
|  | | | | | | | | |
| Identify final timetabled piece of assessment (component and element) | | | | | A1 | | | |
| **% weighting between components A and B** (Standard modules only) | | | | | | | **A:** | **B**: |
| **60%** | **40%** |
|  | | | | | | | | |
| **First Sit** | | | | | | | | |
| **Component A**  **Description of each element** | | | | | | | **Element weighting**  **(as % of component)** | |
| 1. Practical workbook | | | | | | | 100% | |
| **Component B**  **Description of each element** | | | | | | | **Element weighting**  **(as % of component)** | |
| 1. Report (1500 words) | | | | | | | 100% | |
| **Resit (further attendance at taught classes is not required)** | | | | | | | | |
| **Component A**  **Description of each element** | | | | | | | **Element weighting (as % of component)** | |
| 1. Practical workbook | | | | | | | 100% | |
| **Component B  Description of each element** | | | | | | | **Element weighting (as % of component)** | |
| 1. Report (1500 words) | | | | | | | 100% | |
|  | | | | | | | | |
| **Part 4: Learning Outcomes & KIS Data** | | | | | | | | |
| **Learning Outcomes** | On successful completion of this module students will be able to:  Manage intrusion response, including with 3rd parties (Component A)  Organise testing & investigation work in accordance with legal & ethical requirements (Component A and B)  Develop & apply information security policy to implement legal or regulatory requirements (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* |
|  |  |  |
|  |  |  |
|  |  |  |