**THE INTERNATIONAL QUALIFICATIONS**

**AND ASSESSMENT CENTRE (IQAC)**

**«Approved»**

**2025 y. «16» iyul**

| | | | |
|---|---|---|---|
| **Programme** | **LEVEL 5 EXTENDED DIPLOMA IN CYBER SECURITY** | | |
| **Unit Number/ Unit Title** | **UNIT 2 CYBERSECURITY POLICIES AND GOVERNANCE** | | |
| **Cohort Code:** | L04CSP-U2 | | |
| **Unit Level** | Level 4 | | |
| **Total GLH** | Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110 | | |
| **Credits** | 20 CATS/ 10 ECTS | | |
| **Lecturer** | | | |
| **Start Date** | | **End Date** | |

| | |
|---|---|
| **Unit Aims** | This unit aims to provide students with the knowledge and skills to develop, implement, and manage effective cyber security policies and governance frameworks. Students will learn the principles of cyber security policies, understand legal and regulatory requirements, and explore best practices for protecting organizational assets and mitigating cyber risks. |
| **Differentiation Strategies**<br>*(e.g. planned activities or support for individual learners according to their needs)* | The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of sources. Various approaches to addressing the various identified students' needs will be adopted throughout the lesson. Such will include:<br>1. Progressive tasks<br>2. Digital resources<br>3. Verbal support |

| | |
|---|---|
| | 4. Variable outcomes<br>5. Collaborative learning<br>6. Ongoing assessment<br>7. Flexible-pace learning |
| **Equality & Diversity** | Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met. |
| **Safeguarding & Prevent** | Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff. |
| **Health & Safety** | SIRM H&S policies will be maintained. |
| **Learning Resources** | **Teaching and Learning Materials**<br>• Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.<br>• Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional.<br>• Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. |

| Learning Outcome | Assessment Criteria |
|---|---|
| **LO1. Understand fundamental concepts and principles of cyber security** | 1.1 : Explain key concepts, terminologies, and principles of cyber security<br>1.2 Identify common cyber threats and vulnerabilities.<br>1.3 Demonstrate knowledge of basic cyber security tools and techniques. |
| **LO2. Develop skills to identify and mitigate cyber security risks.** | 2.1 : Conduct risk assessments to identify potential security threats.<br>2.2 : Develop risk mitigation strategies and response plans.<br>2.3 : Apply best practices for incident response and recovery. |
| **LO3. Develop effective communication skills in English, both orally and in writing, to convey ideas clearly and coherently, fostering intercultural understanding and empathy.** | 3.1 : Write coherent and well-organized reports and essays demonstrating an understanding of cyber security topics.<br>3.2 : Articulate ideas clearly and effectively in spoken English during presentations and discussions.<br>3.3 : Use appropriate communication strategies for different contexts, including technical and non-technical audiences. |
| **LO4. Employ communication technologies effectively.** | 4.1 : Utilize communication technologies, such as email, video conferencing, and collaboration tools, for efficient business communication.<br>4.2 : Evaluate the advantages and disadvantages of different communication technologies.<br>4.3 : Demonstrate proficiency in using digital communication platforms. |
| **LO5. Navigate cross-cultural communication challenges.** | 5.1 : Recognize and adapt to cross-cultural communication differences in a global business context.<br>5.2 : Develop strategies for effective cross- cultural communication in diverse work environments.<br>5.3 : Identify potential cultural barriers and implement solutions for successful communication. |

| No | Learning Outcome / Topic | Learning and Teaching Activities | Which assessment criteria does the session relate to? | Day/month/ year/ signature |
|---|---|---|---|---|
| 1 | **Core Principles of Cyber Security** | **Core Principles of Cyber Security** CIA Triad (Confidentiality, Integrity, Availability) | LO1: Cyber Security Fundamentals | |
| 2 | **Cyber Security Terminologies** | **Cyber Security Terminologies** Threats, vulnerabilities, risks, attack vectors | LO1: Cyber Security Fundamentals | |
| 3 | **Common Cyber Threats** | **Common Cyber Threats** Malware, phishing, DDoS, insider threats | LO1: Cyber Security Fundamentals | |
| 4 | **Vulnerability Management** | **Vulnerability Management** CVE database, patch management, zero-day exploits | LO1: Cyber Security Fundamentals | |
| 5 | **Basic Security Tools** | **Basic Security Tools** Firewalls, antivirus, VPNs, password managers | LO1: Cyber Security Fundamentals | |
| 6 | **Risk Assessment Frameworks** | **Risk Assessment Frameworks** NIST RMF, ISO 27005, qualitative vs. quantitative analysis | LO2: Risk Management & Mitigation | |
| 7 | **Threat Modeling** | **Threat Modeling** STRIDE, DREAD methodologies | LO2: Risk Management & Mitigation | |
| 8 | Half-Term Exam | - Review of LO1 topics<br>- Practice questions and mock assessment | LO1 LO2 | |
| 9 | **Risk Mitigation Strategies** | **Risk Mitigation Strategies** Avoidance, transfer, acceptance, mitigation | LO2: Risk Management & Mitigation | |

| | | | | |
|---|---|---|---|---|
| **10** | **Incident Response Plans** | **Incident Response Plans** NIST SP 800-61 (Preparation → Post-incident) | LO2: Risk Management & Mitigation | |
| **11** | **Disaster Recovery & BCP** | **Disaster Recovery & BCP** RTO/RPO, backup strategies, failover systems | LO2: Risk Management & Mitigation | |
| **12** | **Cyber Security Policies** | **Cyber Security Policies** Acceptable use, BYOD, remote access policies | LO3: Policy Development & Governance | |
| **13** | **Access Control Models** | **Access Control Models** RBAC, ABAC, least privilege principle | LO3: Policy Development & Governance | |
| **14** | Review | - Comprehensive review of all learning outcomes<br>- Practice questions and revision of key topics | | |
| **15** | Midterm | - **Midterm assessment** covering all learning outcomes (theory and practical elements) | | |
| **16** | Feedback & Reflection | - Review<br>- Individual feedback on performance<br>- Reflective discussion on key learning points | | |
| **17** | **Compliance Standards** | **Compliance Standards** GDPR, HIPAA, PCI-DSS, SOX | LO3: Policy Development & Governance | |
| **18** | **Security Audits & Assessments** | **Security Audits & Assessments** Internal vs. external audits, penetration testing | LO3: Policy Development & Governance | |

| | | | | |
|---|---|---|---|---|
| **19** | **Governance Frameworks** | **Governance Frameworks** COBIT, NIST CSF, ISO 27001 | LO3: Policy Development & Governance | |
| **20** | **Technical Report Writing** | **Technical Report Writing** Structure, clarity, referencing (APA/IEEE) | LO4: Communication & Reporting | |
| **21** | **Executive Summaries** | **Executive Summaries** Translating technical risks for non-technical stakeholders | LO4: Communication & Reporting | |
| **22** | **Presentation Skills** | **Presentation Skills** Visual aids, audience adaptation, Q&A handling | LO4: Communication & Reporting | |
| **23** | Half-Term Exam | **Project** Design a governance framework for a multinational company | | |
| **24** | **Cross-Cultural Communication** | **Cross-Cultural Communication** High-context vs. low-context cultures, global teams | LO4: Communication & Reporting | |
| **25** | **Digital Communication Tools** | **Digital Communication Tools** Secure email (PGP), encrypted messaging (Signal), collaboration (Slack/MS Teams) | LO4: Communication & Reporting | |
| **26** | **Case Study: Data Breach Response** | **Case Study: Data Breach Response** Equifax, SolarWinds incident analysis | LO5: Practical Application & Ethics | |
| **27** | **Policy Drafting Workshop** | **Policy Drafting Workshop** Develop a GDPR-compliant data protection policy | LO5: Practical Application & Ethics | |
| **28** | **Role-Play: Incident Response** | **Role-Play: Incident Response** Mock tabletop exercise (ransomware attack) | LO5: Practical Application & Ethics | |
| **29** | Final Exam Preparation & Review | LO1, LO2, LO3, LO4 | LO1, LO2, LO3, LO4 | |

| | | | | |
|---|---|---|---|---|
| **30** | Final Exam | | LO1, LO2, LO3, LO4 | |