INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

Approved

2025 y. «16» Eylul

Programme	**LEVEL 5 EXTENDED DIPLOMA IN CYBER SECURITY**		
Unit Number/ Unit Title	**UNIT 11 CLOUD SECURITY**		
Cohort Code:	L05CLS-U11		
Unit Level	Level 5		
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	To provide students with a comprehensive understanding of cloud security, including the principles, challenges, and best practices for securing cloud environments. This module covers various aspects of cloud security, from data protection to compliance requirements.
Differentiation Strategies *(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:- 1. Progressive tasks 2. Digital resources 3. Verbal support 4. Variable outcomes

	5. Collaborative learning 6. Ongoing assessment 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** • "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif. • "Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)" by Michael J. Kavis. • "Cloud Security: A Comprehensive Guide to Secure Cloud Computing" by Ronald L. Krutz and Russell Dean Vines. • Viega, J., & McGraw, G. (2001). "Building Secure Software: How to Avoid Security Problems the Right Way." Addison-Wesley Professional. • "Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems" by Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea, and Adam Stubblefield.

Learning Outcome	Assessment Criteria
LO1. Understand the principles and concepts of cloud computing and security models.	**1. Written Assessments:** 1.1 Explain the fundamental principles of cloud computing and different cloud service models (IaaS, PaaS, SaaS). 1.2 Describe the security challenges specific to cloud environments and their implications. 1.3 Identify key components of cloud security architecture.
LO2. 2. Evaluate cloud service provider security measures and practices.	**2. Research Assessments:** 2.1 Conduct research on different cloud service providers' security measures and practices. 2.2 Analyze and compare security features offered by various cloud providers. 2.3 Assess the effectiveness of cloud provider security certifications and compliance with industry standards.
LO3. 3. Implement security controls for data protection and access management in the cloud.	**3. Practical Assessments:** 3.1 Implement data encryption techniques for protecting sensitive information in cloud storage. 3.2 Design and implement access control policies and mechanisms in a simulated cloud environment. 3.3 Evaluate the security implications of data residency and sovereignty requirements in cloud deployments.
LO4. 4. Design and evaluate cloud security architectures and strategies.	**4. Case Study Assessments:** 4.1 Analyze case studies of cloud security breaches and identify vulnerabilities in cloud architectures. 4.2 Develop and justify recommendations for enhancing cloud security postures. 4.3 Design a secure cloud architecture that meets specific organizational requirements and compliance standards.
LO5. 5. Understand compliance and regulatory considerations in cloud security.	**5. Written Assessments:** 5.1 Explain the importance of compliance frameworks (e.g., GDPR, HIPAA) in cloud security. 5.2 Evaluate the impact of regulatory requirements on cloud security practices and policies. 5.3 Discuss strategies for ensuring compliance with relevant regulations when implementing cloud solutions.

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Cloud Computing**	**Introduction to Cloud Computing** Definition, evolution, and business drivers for cloud adoption.	LO1: Principles & Concepts of Cloud Security **(Written Assessments)**	
2	**Cloud Service Models**	**Cloud Service Models** IaaS, PaaS, SaaS: Characteristics, use cases, and security responsibilities.	LO1: Principles & Concepts of Cloud Security **(Written Assessments)**	
3	**Cloud Deployment Models**	**Cloud Deployment Models** Public, private, hybrid, and multi-cloud: Security trade-offs.	LO1: Principles & Concepts of Cloud Security **(Written Assessments)**	
4	**Cloud Security Challenges**	**Cloud Security Challenges** Shared responsibility model, data breaches, misconfigurations, insider threats.	LO1: Principles & Concepts of Cloud Security **(Written Assessments)**	
5	**Cloud Security Architecture**	**Cloud Security Architecture** Key components (firewalls, IAM, encryption, logging) and design principles.	LO1: Principles & Concepts of Cloud Security **(Written Assessments)**	
6	**Threat Landscape for Cloud**	**Threat Landscape for Cloud** DDoS, API vulnerabilities, account hijacking, and supply chain attacks.	LO1: Principles & Concepts of Cloud Security **(Written Assessments)**	
7	**Cloud Provider Security Offerings**	**Cloud Provider Security Offerings** AWS, Azure, GCP: Built-in security tools and shared responsibility matrices.	LO2: Cloud Provider Security Evaluation **(Research Assessments)**	

8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Comparing Cloud Security Features**	**Comparing Cloud Security Features** Encryption options, DDoS protection, identity management across providers.	LO2: Cloud Provider Security Evaluation **(Research Assessments)**	
10	**Cloud Security Certifications**	**Cloud Security Certifications** ISO 27017, SOC 2, FedRAMP: Importance and evaluation criteria.	LO2: Cloud Provider Security Evaluation **(Research Assessments)**	
11	**Third-Party Risk Management**	**Third-Party Risk Management** Assessing CSP compliance with industry standards (NIST, CIS benchmarks).	LO2: Cloud Provider Security Evaluation **(Research Assessments)**	
12	**Cloud SLA Analysis**	**Cloud SLA Analysis** Evaluating uptime guarantees, data ownership clauses, and breach notifications.	LO2: Cloud Provider Security Evaluation **(Research Assessments)**	
13	**Emerging Trends in Cloud Security**	**Emerging Trends in Cloud Security** Confidential computing, serverless security, and AI-driven threat detection.	LO2: Cloud Provider Security Evaluation **(Research Assessments)**	
14	Review	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15	Midterm	- **Midterm assessment** covering all learning outcomes (theory and practical elements)		

16	Feedback & Reflection	- Review - Individual feedback on performance - Reflective discussion on key learning points		
17	**Data Encryption in the Cloud**	**Data Encryption in the Cloud** Implementing client-side vs. server-side encryption (AWS KMS, Azure Key Vault).	LO3: Data Protection & Access Management **(Practical Assessments)**	
18	**Access Control Mechanisms**	**Access Control Mechanisms** Role-Based Access Control (RBAC), ABAC, and least privilege policies.	LO3: Data Protection & Access Management **(Practical Assessments)**	
19	**Identity & Authentication**	**Identity & Authentication** Multi-Factor Authentication (MFA), SSO, and directory services (Azure AD, Okta).	LO3: Data Protection & Access Management **(Practical Assessments)**	
20	**Data Residency & Sovereignty**	**Data Residency & Sovereignty** Legal implications and technical controls for geo-restrictions.	LO3: Data Protection & Access Management **(Practical Assessments)**	
21	**Secure Data Transfer**	**Secure Data Transfer** TLS, VPNs, and direct connect options for hybrid clouds.	LO3: Data Protection & Access Management **(Practical Assessments)**	
22	**Monitoring & Auditing**	**Monitoring & Auditing** Configuring CloudTrail (AWS), Azure Monitor, and SIEM integrations.	LO3: Data Protection & Access Management **(Practical Assessments)**	
23	**Review**	**Cloud Breach Case Studies** Capital One, SolarWinds: Architectural flaws and mitigation strategies.		

24	**Zero Trust for Cloud**	**Zero Trust for Cloud** Micro-segmentation, SDP, and continuous verification in cloud networks.	LO4: Cloud Security Architecture & Strategies **(Case Study Assessments)**	
25	**Secure Cloud Migration**	**Secure Cloud Migration** Lift-and-shift vs. re-architecture: Security considerations.	LO4: Cloud Security Architecture & Strategies **(Case Study Assessments)**	
26	**Disaster Recovery & Backup**	**Disaster Recovery & Backup** Designing RTO/RPO-aligned strategies with AWS Backup/Azure Site Recovery.	LO4: Cloud Security Architecture & Strategies **(Case Study Assessments)**	
27	**Major Compliance Frameworks**	**Major Compliance Frameworks** GDPR, HIPAA, PCI-DSS: Cloud-specific requirements and penalties.	LO5: Compliance & Regulatory Considerations **(Written Assessments)**	
28	**Cloud Governance Strategies**	**Cloud Governance Strategies** Policy as Code (PaC), CSPM tools, and continuous compliance monitoring.	LO5: Compliance & Regulatory Considerations **(Written Assessments)**	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	