INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «__» _____

Programme	**CYBER SECURITY DIPLOMA - LEVEL 6**		
Unit Number/ Unit Title	**UNIT 1 SECURITY ARCHITECTURE AND ENTERPRISE INFRASTRUCTURE**		
Cohort Code:	L06SAEI-U1		
Unit Level	Level 6		
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 module provides learners with advanced knowledge and practical skills required to design and implement secure enterprise-level infrastructure. Emphasis is placed on integrating security principles into on-premise, cloud, and hybrid environments, considering modern threat landscapes, scalability, and compliance requirements. It prepares learners for roles such as Security Engineer, Security Analyst, and Security Consultant.
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** • Sherwood, J., Clark, A., & Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach. CRC Press. • Stallings, W. (2020). Network Security Essentials: Applications and Standards (6th ed.). Pearson. • AWS (2023). AWS Well-Architected Framework: Security Pillar. Amazon Web Services. • The Open Group. (2018). TOGAF® Version 9.2. The Open Group. • NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology.

Learning Outcome	Assessment Criteria
LO1. 1. Evaluate enterprise security requirements and architectural frameworks.	1.1 Critically assess organizational needs to determine appropriate security architecture models 1.2 Compare and contrast leading security architecture frameworks (e.g., SABSA, TOGAF, Zero Trust)
LO2. 2. Design secure and scalable network infrastructures.	2.1 Create a secure network design that incorporates segmentation, defense-in-depth, and access controls 2.2 Justify design decisions using performance, scalability, and threat mitigation criteria.
LO3. 3 Integrate security controls across hybrid and cloud-based systems	3.1 Implement layered security controls in hybrid cloud environments (e.g., AWS, Azure). 3.2 Identify and address common misconfigurations and risks in enterprise cloud infrastructure.
LO4. 4. Assess and enhance the effectiveness of enterprise security architectures	4.1 Conduct vulnerability assessments and architecture reviews to evaluate control effectiveness. 4.2 Recommend improvements based on industry benchmarks and audit findings.
LO5. 5. Apply secure design principles in system development and lifecycle management	5.1 Integrate security into each phase of the system development life cycle (SDLC) 5.2 Develop a security architecture documentation set for enterprise stakeholders.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Security Architecture**	**Introduction to Security Architecture** Role in enterprise risk management, alignment with business objectives.	LO1: Enterprise Security Requirements & Architectural Frameworks	
2	**Assessing Organizational Security Needs**	**Assessing Organizational Security Needs** Stakeholder interviews, risk appetite analysis, compliance mapping (GDPR, HIPAA).	LO1: Enterprise Security Requirements & Architectural Frameworks	
3	**Security Architecture Frameworks: SABSA**	**Security Architecture Frameworks: SABSA** Business-driven approach, layered model (Conceptual to Operational).	LO1: Enterprise Security Requirements & Architectural Frameworks	
4	**Security Architecture Frameworks: TOGAF ADM**	**Security Architecture Frameworks: TOGAF ADM** Integrating security into The Open Group Architecture Framework.	LO1: Enterprise Security Requirements & Architectural Frameworks	
5	**Zero Trust Architecture (ZTA)**	**Zero Trust Architecture (ZTA)** Principles (never trust, always verify), micro-segmentation, identity-centric controls.	LO1: Enterprise Security Requirements & Architectural Frameworks	
6	**Comparative Analysis of Frameworks**	**Comparative Analysis of Frameworks** Use cases for SABSA vs. TOGAF vs. Zero Trust in different industries.	LO1: Enterprise Security Requirements & Architectural Frameworks	
7	**Network Security Fundamentals**	**Network Security Fundamentals** Defense-in-depth, CIA triad, and perimeter vs. zero-trust models.	LO2: Secure Network Infrastructure Design	

8	Review	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Secure Network Segmentation**	**Secure Network Segmentation** VLANs, software-defined perimeters (SDP), and least privilege zoning.	LO2: Secure Network Infrastructure Design	
10	**Access Control Strategies**	**Access Control Strategies** NAC (Network Access Control), RBAC/ABAC, and 802.1X authentication.	LO2: Secure Network Infrastructure Design	
11	**Scalable Network Design** considerations.	**Scalable Network Design** Load balancing, HA (High Availability), and SD-WAN security considerations.	LO2: Secure Network Infrastructure Design	
12	**Threat-Centric Design**	**Threat-Centric Design** Mitigating DDoS, lateral movement, and insider threats via architecture.	LO2: Secure Network Infrastructure Design	
13	**Case Study: Enterprise Network Redesign**	**Case Study: Enterprise Network Redesign** Evaluating trade-offs between performance, cost, and security.	LO2: Secure Network Infrastructure Design	
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	**Hybrid Cloud Security Challenges**	**Hybrid Cloud Security Challenges** Shared responsibility model, data sovereignty, and shadow IT risks.	LO3: Hybrid & Cloud Security Integration	
18	**IAM for Cloud Environments**	**IAM for Cloud Environments** Federated identities (SAML/OIDC), cross-cloud access management.	LO3: Hybrid & Cloud Security Integration	

19	**Cloud Network Security**	**Cloud Network Security** NSGs (Azure), Security Groups (AWS), and cloud-native firewalls.	LO3: Hybrid & Cloud Security Integration	
20	**Common Cloud Misconfigurations**	**Common Cloud Misconfigurations** Exposed S3 buckets, overly permissive IAM roles, and logging gaps.	LO3: Hybrid & Cloud Security Integration	
21	**Secure Cloud Connectivity**	**Secure Cloud Connectivity** VPNs, Direct Connect (AWS), ExpressRoute (Azure), and TLS policies.	LO3: Hybrid & Cloud Security Integration	
22	**Automating Cloud Security**	**Automating Cloud Security** Infrastructure as Code (IaC) security (Terraform, CloudFormation).	LO3: Hybrid & Cloud Security Integration	
23	Half-Term Exam	**Architecture Review Methodologies** Using NIST SP 800-154, ISO 27034 for control evaluation.	LO4: Security Architecture Assessment & Improvement	
24	**Vulnerability Assessments**	**Vulnerability Assessments** Scanning tools (Nessus, Qualys), architectural threat modeling (STRIDE).	LO4: Security Architecture Assessment & Improvement	
25	**Benchmarking & Audits**	**Benchmarking & Audits** CIS Benchmarks, SOC 2 reports, and gap analysis.	LO4: Security Architecture Assessment & Improvement	
26	**Remediation Strategies**	**Remediation Strategies** Prioritizing fixes using risk scoring (CVSS, DREAD).	LO4: Security Architecture Assessment & Improvement	
27	**Security in SDLC Phases**	**Security in SDLC Phases** Requirements (security thresholds), design (threat models), testing (SAST/DAST).	LO5: Secure Design in SDLC & Documentation	
28	**Architecture Documentation**.	**Architecture Documentation** Creating artifacts: network diagrams, control matrices, and compliance reports.	LO5: Secure Design in SDLC & Documentation	

29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	