INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «____» _____

Programme	**CYBER SECURITY DIPLOMA - LEVEL 6**		
Unit Number/ Unit Title	**UNIT 4 CYBER SECURITY GOVERNANCE, COMPLIANCE AND RISK MANAGEMENT**		
Cohort Code:	L06CSGC-U4		
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 unit focuses on building strategic knowledge in risk management, regulatory compliance, and governance frameworks. It prepares learners to take on supervisory or leadership roles requiring oversight of organisational cybersecurity posture and risk mitigation strategies.
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** • ISO/IEC 27001:2022 — International Standard. • NIST SP 800 Series (esp. 800-37, 800-53) • Calder, A. (2022). IT Governance: An International Guide. Kogan Page. • Peltier, T. (2016). Information Security Risk Analysis. CRC Press. • European Union Agency for Cybersecurity (ENISA) Reports

Learning Outcome	Assessment Criteria
LO1. Understand key governance frameworks (e.g., COBIT, ISO 27001).	**Written Report:** 1.1 Compare international cybersecurity governance models. 1.2 Assess the role of ISMS and internal controls
LO2. Evaluate regulatory compliance obligations and enforcement.	**Case Study:** 2.1 Interpret GDPR, PCI-DSS, NIS2 compliance for an organisation. 2.2 Identify penalties and reporting procedures.
LO3. Conduct risk assessments using structured methodologies.	**Project-Based Assignment:** 3.1 Use NIST RMF or ISO 31000 to assess cyber risks. 3.2 Develop a risk treatment plan
LO4. Integrate business continuity and incident management in governance.	**Portfolio Submission:** 4.1 Draft incident response policies. 4.2 Analyse a business continuity strategy for cyber resilience.
LO5. Engage stakeholders in a security governance culture.	**Group Presentation:** 5.1 Communicate risk to non-technical stakeholders. 5.2 Recommend governance models for large organisations.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Cybersecurity Governance**	**Introduction to Cybersecurity Governance**: Principles, objectives, and business alignment.	LO1: Governance Frameworks & Internal Controls	
2	**COBIT Framework**	**COBIT Framework**: Components (Governance vs. Management), maturity models, and implementation.	LO1: Governance Frameworks & Internal Controls	
3	**ISO/IEC 27001**	**ISO/IEC 27001**: ISMS requirements, risk-based approach, and certification process.	LO1: Governance Frameworks & Internal Controls	
4	**NIST Cybersecurity Framework (CSF)**	**NIST Cybersecurity Framework (CSF)**: Core functions (Identify, Protect, Detect, Respond, Recover).	LO1: Governance Frameworks & Internal Controls	
5	**SANS Critical Security Controls**	**SANS Critical Security Controls**: Prioritized safeguards for threat mitigation.	LO1: Governance Frameworks & Internal Controls	
6	**Internal Controls & Audits**	**Internal Controls & Audits**: Role of segregation of duties (SoD), access controls, and SOC reports.	LO1: Governance Frameworks & Internal Controls	
7	**GDPR Deep Dive**	**GDPR Deep Dive**: Data subject rights, DPO roles, and breach notification (72-hour rule).	LO2: Regulatory Compliance & Enforcement	
8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	

9	**PCI-DSS**	**PCI-DSS**: Requirements for cardholder data (encryption, logging, vulnerability scans).	LO2: Regulatory Compliance & Enforcement	
10	**NIS2 Directive**	**NIS2 Directive**: Scope, incident reporting, and supply chain security for critical entities.	LO2: Regulatory Compliance & Enforcement	
11	**HIPAA & CCPA**	**HIPAA & CCPA**: Sector-specific mandates (healthcare, consumer privacy).	LO2: Regulatory Compliance & Enforcement	
12	**Regulatory Penalties & Case Studies**	**Regulatory Penalties & Case Studies**: GDPR fines (e.g., Meta, British Airways), PCI non-compliance costs.	LO2: Regulatory Compliance & Enforcement	
13	**Cross-Border Compliance Challenges**	**Cross-Border Compliance Challenges**: Conflicts between EU/US/APAC regulations (e.g., SchremsII).	LO2: Regulatory Compliance & Enforcement	
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	**Risk Management Fundamentals**	**Risk Management Fundamentals**: Terminology (assets, threats, vulnerabilities, impact).	LO3: Risk Assessment & Treatment	
18	**NIST Risk Management Framework (RMF)**	**NIST Risk Management Framework (RMF)**: Steps from categorization to continuous monitoring.	LO3: Risk Assessment & Treatment	
19	**ISO 31000**	**ISO 31000**: Risk identification, analysis, evaluation, and treatment strategies.	LO3: Risk Assessment & Treatment	

20	**FAIR Model**	**FAIR Model**: Quantitative risk analysis (loss magnitude, probability).	LO3: Risk Assessment & Treatment	
21	**Risk Treatment Plans**	**Risk Treatment Plans**: Mitigation (controls), transfer (insurance), acceptance, and avoidance.	LO3: Risk Assessment & Treatment	
22	**Third-Party Risk Management (TPRM)**	**Third-Party Risk Management (TPRM)**: Vendor assessments and contractual obligations.	LO3: Risk Assessment & Treatment	
23	**Review**	**Communicating Risk to Executives**: Metrics (ROI, ALE), dashboards, and board-level reporting.	LO4: Incident Response & Business Continuity	
24	**Incident Response (IR) Lifecycle**	**Incident Response (IR) Lifecycle**: Preparation, detection, containment, eradication, recovery.	LO4: Incident Response & Business Continuity	
25	**IR Policy Development**	**IR Policy Development**: Roles (CIRT team), communication plans, and legal considerations.	LO4: Incident Response & Business Continuity	
26	**Business Impact Analysis (BIA)**	**Business Impact Analysis (BIA)**: RTO, RPO, and critical system prioritization.	LO4: Incident Response & Business Continuity	
27	**Disaster Recovery (DR) & Cyber Resilience**	**Disaster Recovery (DR) & Cyber Resilience**: Backup strategies, failover systems, and tabletop exercises.	LO4: Incident Response & Business Continuity	
28	**Building a Security Culture**	**Building a Security Culture**: Training programs, phishing simulations, and KPIs for behavioral change.	LO5: Stakeholder Engagement & Security Culture	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	