INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y.«16» 05

Programme	CYBER SECURITY DIPLOMA - LEVEL 7		
Unit Number/ Unit Title	**UNIT 5 GLOBAL CYBER LAW, ETHICS, AND REGULATORY COMPLIANCE**		
Cohort Code:	L07GCLE-U5		
Unit Level	Level 7		
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 addresses global and regional cyber law frameworks, ethics in cyber operations, and regulatory compliance. Learners will compare and contrast laws such as GDPR, HIPAA, and NIS2, while analyzing the implications of cross-border data governance and national security agendas.
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** • Solove, D. J. & Schwartz, P. M. (2020). Information Privacy Law. • Kesan, J. (2019). Cybersecurity and Legal Compliance. • European Union Agency for Cybersecurity (ENISA) Reports. • US NIST and HIPAA Compliance Guidance. • UN GGE Reports on Cyber Norms.

Learning Outcome	Assessment Criteria
LO1. 1. Compare major global and regional cyber laws.	1.1 Analyze GDPR, HIPAA, CCPA, and NIS2 requirements. 1.2 Examine enforcement mechanisms and legal precedents.
LO2. 2. Evaluate ethical issues in cyber security operations.	2.1 Design realistic red team campaigns targeting organizational systems. 2.2 Evaluate tactics, techniques, and procedures (TTPs) using ATT&CK Matrix.
LO3. 3. Develop compliance strategies for organizations.	3.1 Design risk-based compliance plans based on regulatory requirements. 3.2 Evaluate internal audit processes and documentation.
LO4. **4. Interpret cross-border legal complexities.**	4.1 Discuss jurisdictional conflicts in cloud and data transfer cases. 4.2 Analyze data sovereignty vs. global operations.
LO5. 5. Critically assess the role of law in cyber deterrence.	5.1 Evaluate treaties and norms of behavior in cyberspace. 5.2 Propose policy recommendations to strengthen legal deterrence.

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Cyber Law Frameworks**	**Introduction to Cyber Law Frameworks** – Key concepts and jurisdictional challenges	LO1: Compare major global and regional cyber laws	
2	**GDPR Deep Dive**	**GDPR Deep Dive** – Principles, data subject rights, and breach notification	LO1: Compare major global and regional cyber laws	
3	**HIPAA & Healthcare Compliance**	**HIPAA & Healthcare Compliance** – PHI protection, BAAs, and enforcement cases	LO1: Compare major global and regional cyber laws	
4	**CCPA vs. Other U.S. State Laws**	**CCPA vs. Other U.S. State Laws** – CPRA, VCDPA, and emerging trends	LO1: Compare major global and regional cyber laws	
5	**NIS2 Directive (EU)**	**NIS2 Directive (EU)** – Critical infrastructure obligations and reporting	LO1: Compare major global and regional cyber laws	
6	**APAC Cyber Laws**	**APAC Cyber Laws** – China's DSL, Singapore's PDPA, India's DPDP Act	LO1: Compare major global and regional cyber laws	
7	**Ethical Hacking vs. Malicious Hacking**	**Ethical Hacking vs. Malicious Hacking** – Legal boundaries and gray areas	LO2: Evaluate ethical issues in cybersecurity operations	

8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Responsible Vulnerability Disclosure**	**Responsible Vulnerability Disclosure** – Bug bounties, zero-day ethics	LO2: Evaluate ethical issues in cybersecurity operations	
10	**Surveillance & Privacy Trade-offs**	**Surveillance & Privacy Trade-offs** – Government vs. individual rights	LO2: Evaluate ethical issues in cybersecurity operations	
11	**AI Ethics in Cybersecurity**	**AI Ethics in Cybersecurity** – Bias in threat detection, autonomous weapons	LO2: Evaluate ethical issues in cybersecurity operations	
12	**Case Study: Ethical Dilemmas**	**Case Study: Ethical Dilemmas** – Stuxnet, Pegasus spyware, ransomware negotiations	LO2: Evaluate ethical issues in cybersecurity operations	
13	**Debate: Hack-Back Legality**	**Debate: Hack-Back Legality** – Vigilantism or self-defense?	LO2: Evaluate ethical issues in cybersecurity operations	
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-Based Compliance Planning**	**Risk-Based Compliance Planning** – Aligning controls with regulations	LO3: Develop compliance strategies for organizations	
18	**ISO 27001 & SOC 2 Audits**	**ISO 27001 & SOC 2 Audits** – Frameworks for certifying compliance	LO3: Develop compliance strategies for organizations	
19	**Third-Party Vendor Management**	**Third-Party Vendor Management** – Assessing supply chain risks	LO3: Develop compliance strategies for organizations	
20	**Incident Response Legal Preparedness**	**Incident Response Legal Preparedness** – Forensic readiness, litigation holds	LO3: Develop compliance strategies for organizations	
21	**Workshop: Drafting a Compliance Roadmap**	**Workshop: Drafting a Compliance Roadmap** – For a multinational firm	LO3: Develop compliance strategies for organizations	
22	**Internal Audit Simulation**	**Internal Audit Simulation** – Mock audit with findings/remediation	LO3: Develop compliance strategies for organizations	
23	**Review**	**Jurisdictional Conflicts** – Cloud data (Microsoft Ireland case, Schrems II)	LO4: Interpret cross-border legal complexities	
24	**Data Localization Laws**	**Data Localization Laws** – Russia's FZ-152, Vietnam's Decree 53	LO4: Interpret cross-border legal complexities	
25	**Cross-Border E-Discovery**	**Cross-Border E-Discovery** – Legal hurdles in multinational investigations	LO4: Interpret cross-border legal complexities	
26	**Workshop: Data Transfer Mechanisms**	**Workshop: Data Transfer Mechanisms** – SCCs, BCRs, and Privacy Shield 2.0	LO4: Interpret cross-border legal complexities	

27	**International Cyber Norms**	**International Cyber Norms** – UNGGE, Tallinn Manual, Paris Call	LO5: Critically assess the role of law in cyber deterrence	
28	**Policy Debate: Can Laws Deter Cybercrime?**	**Policy Debate: Can Laws Deter Cybercrime?** – Ransomware gangs, state-sponsored APTs	LO5: Critically assess the role of law in cyber deterrence	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	