INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

____

2025 y. «16» iyul ____________

INTERNATIONAL QUALIFICATIONS AND ASSESSMENT CENTRE • XALQARO MALAKALAR VA BAHOLASH MARKAZI • IQAC

Programme	**CYBER SECURITY DIPLOMA - LEVEL 7**		
Unit Number/ Unit Title	**UNIT 1 STRATEGIC CYBER SECURITY LEADERSHIP AND POLICY DEVELOPMENT**		
Cohort Code:	L07SCSL-U1		
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 focuses on equipping learners with the skills to lead cyber security strategy at the organizational and national levels. It explores policy frameworks, strategic planning, security program implementation, and stakeholder engagement. Learners will critically examine the complexities of leadership and the development of cyber security policies within global, governmental, and corporate contexts.
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**
	• Bayuk, J. (2010). Cybersecurity Policy Guidebook. Wiley. • Von Solms, B. & Van Niekerk, J. (2013). "From Information Security to Cyber Security". Computers & Security. • ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. • NIST Cybersecurity Framework (2020). • ISO/IEC 27001:2022 Standard.

Learning Outcome	Assessment Criteria
LO1. 1. Demonstrate an understanding of cyber security leadership models and governance structures.	1.1 Analyse various cyber security leadership frameworks. 1.2 Evaluate the roles of CISOs and senior management in strategy implementation
LO2. 2. Develop cyber security strategies aligned with organizational objectives.	2.1 Design strategic plans integrating risk, compliance, and threat intelligence. 2.2 Assess key performance indicators for strategy effectiveness.
LO3. 3. Formulate cyber security policy at organizational and governmental levels.	3.1 Develop a draft cyber security policy aligned with current legal frameworks. 3.2 Analyse challenges in policy enforcement and cross-border cooperation.
LO4. 4. Evaluate the influence of international standards and frameworks.	4.1 Critically review ISO 27001, NIST CSF, and COBIT. 4.2 Apply frameworks in developing strategic recommendations.
LO5. 5. Engage stakeholders to build a cyber-aware culture.	5.1 Propose communication and training initiatives for executives and employees. 5.2 Analyse stakeholder roles in shaping cyber maturity.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Cybersecurity Leadership Frameworks**	**Cybersecurity Leadership Frameworks** – NIST, SANS, and MITRE leadership models.	LO1: Demonstrate an understanding of cybersecurity leadership models and governance structures.	
2	**Roles of CISOs & Executive Boards**	**Roles of CISOs & Executive Boards** – Responsibilities, reporting lines, and influence.	LO1: Demonstrate an understanding of cybersecurity leadership models and governance structures.	
3	**Governance vs. Management in Cybersecurity**	**Governance vs. Management in Cybersecurity** – Board-level vs. operational oversight.	LO1: Demonstrate an understanding of cybersecurity leadership models and governance structures.	
4	**Public vs. Private Sector Cybersecurity Leadership**	**Public vs. Private Sector Cybersecurity Leadership** – Differences in priorities and constraints.	LO1: Demonstrate an understanding of cybersecurity leadership models and governance structures.	
5	**Case Study: Leadership Failures & Successes**	**Case Study: Leadership Failures & Successes** – Lessons from major breaches (e.g., SolarWinds, Equifax).	LO1: Demonstrate an understanding of cybersecurity leadership models and governance structures.	
6	**Workshop: Designing a Cybersecurity Governance Structure**	**Workshop: Designing a Cybersecurity Governance Structure** – Aligning leadership with organizational needs.	LO1: Demonstrate an understanding of cybersecurity leadership models and governance structures.	
7	**Strategic Planning Process**	**Strategic Planning Process** – From risk assessment to roadmap development.	LO2: Develop cybersecurity strategies aligned with organizational objectives.	

8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Integrating Threat Intelligence into Strategy**	**Integrating Threat Intelligence into Strategy** – Proactive vs. reactive approaches.	LO2: Develop cybersecurity strategies aligned with organizational objectives.	
10	**Balancing Risk, Compliance & Business Goals**	**Balancing Risk, Compliance & Business Goals** – Cost-benefit analysis of security investments.	LO2: Develop cybersecurity strategies aligned with organizational objectives.	
11	**KPIs for Cybersecurity Effectiveness**	**KPIs for Cybersecurity Effectiveness** – Metrics for measuring strategy success (e.g., MTTR, incident rates).	LO2: Develop cybersecurity strategies aligned with organizational objectives.	
12	**Scenario Planning & Cyber Resilience**	**Scenario Planning & Cyber Resilience** – Preparing for emerging threats (AI, quantum computing).	LO2: Develop cybersecurity strategies aligned with organizational objectives.	
13	**Group Exercise: Drafting a Cybersecurity Strategy**	**Group Exercise: Drafting a Cybersecurity Strategy** – Aligning with a given business model.	LO2: Develop cybersecurity strategies aligned with organizational objectives.	
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	**Components of a Cybersecurity Policy**	**Components of a Cybersecurity Policy** – Access control, incident response, data protection.	LO3: Formulate cybersecurity policy at organizational and governmental levels.	
18	**Legal & Regulatory Compliance**	**Legal & Regulatory Compliance** – GDPR, HIPAA, CCPA, and sector-specific laws.	LO3: Formulate cybersecurity policy at organizational and governmental levels.	
19	**Policy Enforcement Challenges**	**Policy Enforcement Challenges** – Employee resistance, shadow IT, BYOD risks.	LO3: Formulate cybersecurity policy at organizational and governmental levels.	
20	**Cross-Border Cybersecurity Cooperation**	**Cross-Border Cybersecurity Cooperation** – Challenges in global policy harmonization.	LO3: Formulate cybersecurity policy at organizational and governmental levels.	
21	**Simulation: Policy Drafting for a Multinational Company**	**Simulation: Policy Drafting for a Multinational Company** – Addressing jurisdictional conflicts.	LO3: Formulate cybersecurity policy at organizational and governmental levels.	
22	**Debate: Privacy vs. Security in Policy-Making**	**Debate: Privacy vs. Security in Policy-Making** – Government surveillance vs. individual rights.	LO3: Formulate cybersecurity policy at organizational and governmental levels.	
23	**Review**	**Comparative Analysis of ISO 27001, NIST CSF & COBIT** – Strengths and limitations.	LO4: Evaluate the influence of international standards and frameworks.	
24	**Adopting Frameworks in Different Sectors**	**Adopting Frameworks in Different Sectors** – Healthcare, finance, critical infrastructure.	LO4: Evaluate the influence of international standards and frameworks.	

25	**Workshop: Applying NIST CSF to a Case Study**	**Workshop: Applying NIST CSF to a Case Study** – Identifying gaps and improvements.	LO4: Evaluate the influence of international standards and frameworks.	
26	**Emerging Standards (e.g., ISO/IEC 23360 for AI Security)**	**Emerging Standards (e.g., ISO/IEC 23360 for AI Security)** – Future-proofing strategies	LO4: Evaluate the influence of international standards and frameworks.	
27	**Stakeholder Mapping & Influence Strategies**	**Stakeholder Mapping & Influence Strategies** – Engaging executives, employees, and third parties. **Designing Awareness Programs** – Phishing simulations, gamification, and metrics for behavior change.	LO5: Engage stakeholders to build a cyber-aware culture.	
28	**Role-Playing: Communicating Cyber Risks to Non-Technical Audiences**	**Role-Playing: Communicating Cyber Risks to Non-Technical Audiences** – Boardroom presentations. **Ethical Leadership & Corporate Social Responsibility (CSR) in Cybersecurity** – Building trust.	LO5: Engage stakeholders to build a cyber-aware culture.	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	