# Week 1: Matching your cyber skills and Form a Group

**Activity 1: Warm-up: Refresh of Graduate Learning Outcomes**

* **Activity**: Participate in a live poll to self-assess your skills in four key areas: Discipline-specific knowledge and capabilities, Digital literacy, Problem solving, and Critical thinking.
* **Discussion**: Think about how you've used these skills in your previous studies or work experiences and how they might be applicable in various professional settings.

|  |  |
| --- | --- |
| GLO1 Discipline-specific knowledge and capabilities |  |
| GLO3 Digital literacy |  |
| GLO4 Critical thinking |  |
| GLO5 Problem solving |  |

**Activity 2: Understanding Cybersecurity Careers and Skill Mapping**

* Reflect on your past work experiences, educational achievements, and personal strengths.
* Think about how these aspects of your background might make you a good fit for roles in cybersecurity.
* Use the provided materials to match your experiences and attributes to the requirements of the role.

|  |  |
| --- | --- |
|  | CYBER SECURITY GOVERNANCE & RISK MANAGEMENT |
| Personal attributes | * taking account of multiple complex factors to arrive at logical, repeatable conclusions * verbal and written communication, especially in producing formal documents which are comprehensive and without ambiguities * presenting logical, objective reasons for all decisions made * encouraging and supporting colleagues, including those in other departments, to achieve shared objectives * working effectively within organisational policies, procedures, and security and legal constraints * being sensitive and constructive when challenging other people’s ideas or decisions * evaluating the probable social, commercial, cultural, ethical and environmental consequences of an action |
| Specialist skills | * using statistical, mathematical or financial techniques to assess the likelihood (taking account of vulnerabilities and threats) and impact of cyber-attack techniques and deliberate or unintentional damaging actions by people within the organisation * applying risk management methodologies, such as those in ISO 27001, and sector-specific requirements, such as PCI-DSS * interpreting legal and regulatory requirements and integrating them with an organisation’s operational requirements * assessing the compliance of procedures and practice with agreed standards |
| Experience | Any role that develops the abilities to assess complex sets of factors, methodically generate logical conclusions and document these very clearly, could provide a good foundation, with some additional specialist training, for a role in this specialism.  Examples of such careers and roles include:   * roles in the emergency services, especially fire and police services, which require substantial risk management * operational and staff roles in the Armed Forces * business risk management * business operations * IT system management * business continuity * financial or internal audit * specialist commercial insurance assessment |
| Core knowledge | * Risk Management & Governance * Security management systems and organisational security controls |
| Related knowledge | * Law & Regulation * Human Factors * Cyber-Physical Systems |

**Activity 3: Group Formation Based on Diverse Skill Sets**

* **Team Building**: Form groups of 3 and ensure a mix of skills and experiences that match the requirements of cybersecurity role discussed. This diverse skill set can help you better complete AT2!
* **Discussion**: In your groups, discuss the matches you've made and share insights into how your unique experiences might contribute to a career in cybersecurity; Explore the benefits of diverse skills and experiences in creating strong cybersecurity teams.

**Prepare for Week 2 Seminar**

* Please find one good/bad example of security awareness training artifact. We will benchmark it with AT1 marking rubric to help me better understand how to prepare for AT1.