**Cyber Security Specialist**  
Use the following learning outcomes codes to help map your portfolio evidence from both your on-programme University work and work undertaken in the workplace.  
  
You not need to map everything to a learning outcome, just use the ones that are appropriate to your job role your current abilities and skills sets.  
  
**Standard Core Skills (CS)**

|  |  |
| --- | --- |
| CS1 | Information Systems: can critically analyse a business domain to identify the role of information systems, highlight issues and identify opportunities for improvement through evaluating information systems in relation to their intended purpose and effectiveness. |
| CS2 | Systems Development: analyses business and technical requirements to select and specify appropriate technology solutions. Designs, implements, tests, and debugs software to meet requirements using contemporary methods including agile development. Manages the development and assurance of software artefacts applying secure development practises to ensure system resilience. Configures and deploys solutions to end-users. |
| CS3 | Data: identifies organisational information requirements and can model data solutions using conceptual data modelling techniques. Can implement a database solution using an industry standard database management system (DBMS). Can perform database administration tasks and is cognisant of the key concepts of data quality and data security.  Can manage data effectively and undertake data analysis. |
| CS4 | Cyber Security: can undertake a security risk assessment for a simple IT system and propose resolution advice. Can identify, analyse and evaluate security threats and hazards to planned and installed information systems or services (e.g. Cloud services). |
| CS5 | Business Organisation: can apply organisational theory, change management, marketing, strategic practice, human resource management and IT service management to technology solutions development. Develops well- reasoned investment proposals and provides business insights. |
| CS6 | IT Project Management: follows a systematic methodology for initiating, planning, executing, controlling, and closing technology solutions projects. Applies industry-standard processes, methods, techniques, and tools to execute projects. Can manage a project (typically less than six months, no inter-dependency with other projects and no strategic impact) including identifying and resolving deviations and the management of problems and escalation processes. |
| CS7 | Computer and Network Infrastructure: can plan, design and manage computer networks with an overall focus on the services and capabilities that network infrastructure solutions enable in an organisational context. Identify network security risks and their resolution. |

**Core Technical Knowledge Knows and understands (**CTK)**:**

|  |  |
| --- | --- |
| CTK1 | How business exploits technology solutions for competitive advantage. |
| CTK2 | The value of technology investments and how to formulate a business case for a new technology solution, including estimation of both costs and benefits. |
| CTK3 | Contemporary techniques for design, developing, testing, correcting, deploying, and documenting software systems from specifications, using agreed standards and tools. |
| CTK4 | How teams work effectively to produce technology solutions. |
| CTK5 | The role of data management systems in managing organisational data and information. |
| CTK6 | Common vulnerabilities in computer networks including unsecure coding and unprotected networks. |
| CTK7 | The various roles, functions and activities related to technology solutions within an organisation. |
| CTK8 | How strategic decisions are made concerning acquiring technology solutions resources and capabilities including the ability to evaluate the different sourcing options. |
| CTK9 | How to deliver technology solutions project accurately consistent with business needs. |
| CTK10 | The issues of quality, cost and time for projects, including contractual obligations and resource constraints. |

# Core Behavioural Skills (CBS)

|  |  |
| --- | --- |
| Professional, interpersonal, and business skills | |
| CBS1 | Fluent in written communications and able to articulate complex issues. |
| CBS2 | Makes concise, engaging, and well-structured verbal presentations, arguments and explanations. |
| CBS3 | Able to deal with different, competing interests within and outside the organisation with excellent negotiation skills. |
| CBS4 | Can identify the preferences, motivations, strengths and limitations of other people and apply these insights to work more effectively with and to motivate others. |
| CBS5 | Competent in active listening and in leading, influencing, and persuading others. |
| CBS6 | Able to give and receive feedback constructively and incorporate it into your own development and life-long learning. |
| CBS7 | Applies analytical and critical thinking skills to Technology Solutions development and to systematically analyse and apply structured problem-solving techniques to complex systems and situations. |
| CBS8 | Able to put forward, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business need, using open questions and summarising skills and basic negotiating skills. |
| CBS9 | Able to conduct effective research, using literature and other media, into IT and business-related topics. |
| Attributes and behaviours | |
| CBS10 | Have demonstrated that they have mastered basic business disciplines, ethics and courtesies, demonstrating timeliness and focus when faced with distractions and the ability to complete tasks to a deadline with high quality. |
| CBS11 | Flexible attitude. |
| CBS12 | Ability to perform under pressure. |
| CBS13 | A thorough approach to work. |
| CBS14 | Logical thinking and creative approach to problem-solving. |

**Cyber Security Specialist DATs Specialism Outcomes**

A cyber security analyst is responsible for the implementation, maintenance and support of the security controls that protect an organisation’s systems and data assets from threats and hazards. They ensure that security technologies and practices are operating in accordance with the organisation’s policies and standards to provide continued protection. They require a broad understanding of network infrastructure, software and data to identify where threat and hazard can occur. They are responsible for performing periodic vulnerability assessments to evaluate the organisation’s ongoing security posture and will provide visibility to management of the main risks and control status on an ongoing basis. They respond to security incidents and implement resolution activities across the organisation.

**Cyber Security Specialist** Skills - **Be able to:** (CSSS):

|  |  |
| --- | --- |
| CSSS1 | Analyse and evaluate security threats and vulnerabilities to planned and installed information systems or services and identify how these can be mitigated against. |
| CSSS2 | Perform security risk assessments for a range of information systems and propose solutions. |
| CSSS3 | Develop a security case against recognised security threats, and recommend mitigation, security controls and appropriate processes. |
| CSSS4 | Define and justify a user access policy for an information system given knowledge of the system architecture, security requirements and threat/risk environment. This should be in terms of what they can do, resources they can access, and operations they are allowed to perform. |
| CSSS5 | Perform a business impact analysis in response to a security incident and follow a disaster recovery plan to meet elements of a given business continuity policy. |
| CSSS6 | Conduct a range of cyber security audit activities to demonstrate security control effectiveness |

**Cyber Security Specialist Technical Knowledge - Knows and understands (CSSTK):**

|  |  |
| --- | --- |
| **CSS**TK1 | The types of security (confidentiality, authentication; non-repudiation; service integrity) and security big picture (network security; host OS security; physical security). |
| **CSS**TK2 | The main types of common attack techniques, including phishing, social engineering, malware, network interception, blended techniques, denial of service and theft. |
| **CSS**TK3 | How to recognise and assess risk including performing a risk assessment. |
| **CSS**TK4 | How to apply penetration testing effectively and how it contributes to assurance. |
| **CSS**TK5 | The different approaches to risk treatment and management in practice. |
| **CSS**TK6 | The different approaches to risk treatment and management in practice. |