**Competencies**

Name:

Company:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Able?** | **When?** | **Technical Competencies** | **Technical Knowledge and Understanding** | **Mapping** | **Completed** |
|  |  | 1: N/A | Foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance. | 1 |  |
|  |  | 2: Design, build, configure, optimise, test and troubleshoot simple and complex networks. | Network foundations, connections, internetworking, protocols, standards, performance, security and server virtualisation. | 2 |  |
|  |  | 3: Apply statistical techniques to large data sets. Identify vulnerabilities in big data architectures and deployment. | Information management, big data concepts, statistical techniques, database concepts and data quality. | 3 |  |
|  |  | 4: Build test and debug a digital system to a specification. | Computer architecture, digital logic, machine level representation of data. | 1 |  |
|  |  | 5: Configure an Operating System in accordance with security policy. Identify threats and features. | Operating System principles, architectures, features, mechanisms, security features and exploits. | 1 |  |
|  |  | 6: Write, test, debug programs in high and low level languages and scripts. | Algorithm and program design, concepts, compilers and logic. Programming languages. | 3 |  |
|  |  | 7: Design, implement and analyse algorithms. | Algorithms, complexity and discrete maths. | 5, 6 |  |
|  |  | 8: Construct software to interact with the real world and analyse for security exploits. | How software interacts with the hardware and real world environment and security issues. | 3, 7 |  |
|  |  | 9: Analyse malware & identify its mechanisms. | Malware, reverse engineering, obfuscation. | 4 |  |
|  |  | 10: Apply secure programming principles and design patterns to address security issues. | Defensive programming, malware resistance, code analysis, formal methods, good practice. | 3, 4, 8, 9 |  |
|  |  | 11: Apply system engineering and software development methodologies and models. | System development principles, tools, approaches, complexity, software engineering. | 3 |  |
|  |  | 12: Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations. | Threats, vulnerabilities, impacts and mitigations in ICT systems and the enterprise environment. | 4, 11 |  |
|  |  | 13: Assess culture & individual responsibilities. | Human dimensions of cyber security. | 11 |  |
|  |  | 14: Undertake ethical system reconnaissance and intelligence analysis. | Structured and ethical intelligence analysis, methods, techniques. | 9, 10 |  |
|  |  | 15: Undertake risk modelling, analysis and trades. | Management of cyber security risk, tools and techniques. | 10 |  |
|  |  | 16: Undertake risk assessment to an external standard. | Quantitative & qualitative risk management theory & practice, role of risk stakeholders. | 10 |  |
|  |  | 17: Apply a management system and develop an information security management plan. | Concepts & benefits of security management systems, governance & international standards. | 9, 11 |  |
|  |  | 18: Configure and use security technology components and key management. | Security components: how they are used for security / business benefit. Crypto & key management. | 5 |  |
|  |  | 19: Design & evaluate a system to a security case. | How to compose a justified security case. | 9 |  |
|  |  | 20: Architect, analyse & justify a secure system. | Understand security assurance, how to achieve it and how to apply security principles | 9 |  |
|  |  | 21: Develop an assurance strategy. | Assurance concepts & approaches. | 9 |  |
|  |  | 22: Security monitoring, analysis and intrusion detection. Recognise anomalies & behaviours. | How to diagnose cause from observables. Application of SIEM (Security Information and Event Management) tools & techniques. | 4, 10,11 |  |
|  |  | 23: Manage intrusion response, including with 3rd parties. | Cyber incident response, management, escalation, investigation & 3rd party involvement. | 11 |  |
|  |  | 24: N/A | Legal, regulatory, compliance & standards environment. | 11 |  |
|  |  | 25: Organise testing & investigation work in accordance with legal & ethical requirements. | Applicability of laws regulations & ethical standards. | 11 |  |
|  |  | 26: Develop & apply information security policy to implement legal or regulatory requirements. | Legal responsibilities of system owners, users, employers, employees. | 11 |  |
|  |  |  |  |  |  |
| 1 |  | Operating systems and architecture |  |  |  |
| 2 |  | Networking |  |  |  |
| 3 |  | Programming |  |  |  |
| 4 |  | Cyber threats |  |  |  |
| 5 |  | Cryptography, mathematics and algorithms |  |  |  |
| 6 |  | Operating system security and defensive programming |  |  |  |
| 7 |  | Embedded systems security |  |  |  |
| 8 |  | Information management and security |  |  |  |
| 9 |  | Security assurance and security case development |  |  |  |
| 10 |  | Risk and information management |  |  |  |
| 11 |  | Cybersecurity incident management and professionalism |  |  |  |