Occupational Specialism: Cyber Security

Performance Outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data

Knowledge specific to Performance Outcome	Skills specific to Performance Outcome
Principles of organisational information security governance and the components of an organisation's cyber security technical infrastructure including hardware, operating systems, networks, software and cloud Cyber security policies and standards based on an Information Security Management System (ISMS) Types of physical, procedural and technical controls including an understanding of: • a recovery plan • preventative e.g. *Fencing/gate/cage, Separation of duties* • detective *e.g. CCTV, Logs, audit* • corrective *e.g. Fire suppression, Standard operatingprocedure* • deterrent *e.g. security guards, employment contracts* • directive *e.g. sign, Agreement types, general securitypolicies* • compensating *e.g. air conditioning, Role-based awarenesstraining* • how a disaster recovery plan works, *e.g. backups, businesscontinuity* • Cryptography, certificates and use of certificate management tools Awareness of how current legislation relates to or impacts upon the cyber security occupation including Data Protection Act,	Apply and maintain procedures and security controls in the installation, configuration and support of physical and virtual infrastructure to ensure confidentiality, integrity and availability, such as: • set up a small Workgroups environment and apply groups and roles within directory services • set up and apply a certificate authority • implement security controls in a small business environment according to NCSC cyber essentials • manage physical documents in line with the GDPR • set up a simple network and apply access controls Protect personal, physical and environmental security in accordance with legislation, procedures, controls and policies Install software for network and end user devices and network such as servers, firewalls and desktop computers to identify andmitigate vulnerabilities, including: • vulnerability scanning • anti-malware • device hardening Undertake a security risk assessment for a simple system such as a desktop or laptop computer connected to a local area network Demonstrate continuous improvement, such as mitigating

Regulation of Investigatory Powers Act, Human Rights Act, Computer Misuse Act, Freedom of Information Act, Official Secrets Act, Payment Card Industry Data Security Standard (PCIDSS), Wireless and Telegraphy Act, professional body codes of conduct, ethical use of information assets Core terminology of cyber security including confidentiality, integrity, availability (the CIA triad), assurance, authenticity, identification, authentication, authorisation, accountability, reliability, non-repudiation, access control	vulnerabilities, incident response detected in networked equipment, updating devices with the latest releases of security software, and undertaking penetration testing Handle and assess the validity of security requests

Performance Outcome 2: Propose remediation advice for a security risk assessment

Knowledge specific to Performance Outcome	**Skills specific to Performance Outcome**
Computer forensic and compliance principles including the importance of ensuring that evidence is not contaminated and the maintenance of continuity of evidence without compromising it **Threats, sources and identification** • Social engineering *e.g. phishing, spear phishing, vishing, smishing, shoulder surfing, dumpster diving* • Denial of service (DoS)/ Distributed Denial of Service (DDoS) • Malware, *e.g, virus, adware, ransomware, trojan, botnet, spyware o Password attack, for example, brute force, dictionary attack o Man in the Middle* **Vulnerabilities** • components of a vulnerability assessment scope • techniques to evaluate the results of a vulnerability assessment and provide recommendations based upon the evidence provided by the vulnerability assessment tools	Identify and categorise threats, vulnerabilities and risks Contribute to risk assessment through recognition of when and how to escalate information about security events whilst preserving evidence Scope, document and evaluate results of vulnerability assessments Provide recommendations based upon the evidence provided by vulnerability assessment tools Document incident and event information and incident, exception and management reports in line with policies and procedures

• impact that vulnerabilities might have on an organisation
• common vulnerability assessment tools and their strengths and weaknesses
 	
Risk management
• understanding of impact and risk management for the mitigation of threats and vulnerabilities
  ○ types *e.g. Life, Property, Safety, finance, reputation*
  ○ privacy *e.g. breaches to business data which could compromise company confidential information*
  ○ measures e.g. *RTO/RPO, MTBF, MTTR*
  ○ identification of critical systems *e.g. single point of failure, mission essential functions*
• threat assessment *e.g. Environmental, Manmade, Internalexternal*
• risk assessment *e.g. Asset value, Likelihood of occurrence,Supply chain assessment*
• an understanding of Qualitative and Quantitative approaches using tools *such as Fault Tree Analysis, Failure Mode Effect Critical Analysis, Annualised Loss Expectancy and /or CCTA Risk Analysis and ManagementMethodology*
• testing *e.g. Penetration testing authorisation, Vulnerabilitytesting authorisation*
• risk response *e.g. Accept, transfer, avoid, mitigate*
• reporting requirements and how to document incident and event information as part of a chain of evidence
• when and how to escalate information about security events
 	
Design and execution of risk mitigation techniques that are appropriate to the perceived business risk, including:
• technical security controls *using e.g. the 5 Cyber Essentialscontrols*
	Monitor cyber security compliance and provide relevant data from log files and incident reports for *e.g. auditing purposes*

• encryption *using industry standard tools e.g. Windows 10,Apple macOS, for Full Disk Encryption or File encryption and TLS and SSL for data in transit. Knowing when each would be applicable* • backups • *information security policies including the relationships of organisation policiesand procedures in risk mitigation, acceptable use, asset disposal*	

Performance Outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge specific to Performance Outcome	**Skills specific to Performance Outcome**
Sources of knowledge: • reliable and unreliable e.g. internet and search engines, academic papers and peers Evaluation techniques e.g*. objective ways of evaluation such as gap analysis, maturity assessments* Communication methods including *sharing knowledge via digital service and project management tools, appropriate enterprise social media, knowledge bases, wikis, blogs and community forums* Evolving cyber security issues in the digital world including the application to critical national infrastructure, communications technologies, the need for information assurance and governance, control systems and internet of things (IoT) devices	Identify (up to three) sources, *such as Google, stack overflow, Wikipedia,* and assess their reliability Demonstrate the validity and appropriateness of the information and its legitimate use Corroborate across multiple sources *e.g. cross referencing* Search for information relevant to a topic or scenarios *e.g. threat intelligence and common attack techniques, cyber security policies, procedures, guidelines and legislation and industry standards related to the implementation of cyber security in an organisation,*

Knowledge specific to Performance Outcome	Skills specific to Performance Outcome
	Select and use techniques and tools to aid evaluation e.g. formative, summative, observation, user diaries, conclusions, and recommendations Compare options, appraise and recommend actions to ensure reliability of source Identify and understand bias *e.g. materials written by a particular developer such as Microsoft in the context of software development and operating systems* Demonstrate critical thinking e.g. triangulation /evaluation of sources to make the best use of digital technologies