GUIDANCE NOTE

Issued: 1st October 2020

Cyber Security Technologist (ST0124)

END-POINT ASSESSMENT ADDITIONAL GUIDANCE ON SOME OF THE OCCUPATIONAL BRIEF COMPETENCY STANDARDS

The following guidance is designed to support End-Point Assessment Organisations (EPAOs) by providing some clarity to those parts of the occupational brief that have caused uncertainty when assessing and moderating apprenticeship work.

The table shows what the minimum expected requirements are for a pass on some of the criteria listed in the occupational brief and offers guidance on how this could be interpreted. Note that there are other criteria (competency standards) in the occupational brief and this table focuses on just those competency standards EPAOs felt needed further guidance.

This is indicative guidance only and represents an attempt to develop a shared understanding of how the competency standards can be interpreted.

The What – what the apprentice has shown they can do		
Competency Standard	**Minimum, expected, requirements for a pass**	**Comments on assessment**
React to threats, hazards, risks and intelligence	The apprentice should be able to: • Discover (through a mix of research and practical exploration) vulnerabilities in a system. • Analyse and evaluate security threats and hazards to a system or service or processes. Be aware of and demonstrate relevant external sources of threat intelligence or advice (e.g. CERT UK) and combine different sources to create an enriched view. • Research and investigate some common attack techniques and recommend how to defend against them. Be aware of and demonstrate use of relevant external sources of vulnerabilities (e.g. OWASP). • Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.	Practical exploration of vulnerabilities could either be done with a combination of freely available tools or by using a commercial vulnerability scanner. There should be a range of types of vulnerabilities examined. The analysis and evaluation of threats and hazards should be for a real system or one that an employer/client is considering deploying, or a service or process in use by the employer but not a theoretical one. The risk assessment should follow a recognised methodology. A simple system could be an individual computer, an application, a service or business process used by the employer.

Develop and use a security case	The apprentice should be able to: • Source and analyse a security case (e.g. a Common Criteria Protection Profile for a security component) and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern. • Develop a simple security case without supervision. (A security case should describe the security objectives, threats, and for every identified attack technique identify mitigation or security controls that could include technical, implementation, policy or process).	The security case analysed could be an existing one written by an external entity which could be a not-for-profit, academic institution, industry group, government agency or vendor. It could also be a security case written by a senior colleague that would serve the same purpose. When developing a simple security case this could also be for and existing system or one the employer/client is thinking about deploying.
Identify future trends	The apprentice should be able to investigate different views of the future (using more than one external source) and trends in a relevant technology area and describe what this might mean for a business, with supporting reasoning.	The apprentice should use different sources to form a view on the future impact of at least one emerging technology area rather than use one source to write about the current state of multiple technology areas. The business doesn't have to be the employer. However, this may make most sense if the apprentice is relating the future trends to their business. The requirement is for more than one external source and by relating the research to their employer's business, apprentices may identify more than one relevant technology area.

OPTION 1: TECHNOLOGIST

Competency Standard	**Minimum, expected, requirements for a pass**	**Comments on criteria**
Design, build and test a network	The apprentice should be able to: • Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, that includes servers, hubs, switches, routers and user devices to a given design requirement without supervision. • Provide evidence that the system meets the design requirement.	If this cannot be achieved, the apprentice should make it clear that they cannot evidence this particular criterion, as it cannot be carried out in the workplace (e.g. it is a role assigned to more senior members of the team or staff). They will include supporting evidence and justification of this by having the employer validate this situation and they should submit any evidence they have of applying competence albeit it a potentially simulated environment but relating to the workplace. The expectation would then be that the apprentice would select a project that would allow them to demonstrate the ability to 'design, build, test and troubleshoot'. If the normal business practice is to use a virtual environment to design, build and test security in networks then its valid for the apprentice to do the same without it being regarded as a simulation.

Analyse a security case	The apprentice should be able to: • Analyse security requirements (functional and non-functional security requirements that may be presented in a security case) against other design requirements (e.g. usability, cost, size, weight, power, heat, supportability etc.), given for a given system or product. • Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.	The apprentice should analyse requirements for a technical solution that provides a security control or set of controls to address a specific business need. This solution could already be in place or could be one that has been proposed.
Implement security in a network (structured and reasoned)	The apprentice should be able to: • Design and build a simple system in accordance with a simple security case. Provide evidence that the system has properly implemented the security controls required by the security case. The system could be either at the enterprise, network or application layer. • Select and configure at least 2 types of common security hardware and software components to implement a given security policy. • Design a system employing a crypto to meet defined security objectives. Develop and implement a key management plan for the given scenario/system.	The system could be the same solution as the one used in the 'Design, build and test a network' activity. However, you should expect to see a broader range of tools and situations if it is a different activity. Common security hardware or software could include a firewall, a switch, router or VPN from the 'Design, build and test a network' configuring. The key point is the device has to be configured to address a security risk. For example: • Configuring secure shell (SSH) on a switch to provide security for remote connections by providing strong encryption when a device is authenticated and also for the transmitted data between the communicating devices. • Configuring an access control list on a router to filter traffic by stating what is permitted or denied. Note: The apprentice is building a simple system in accordance with a simple security case, as such, they will be using the platforms, technologies and hardware available to them within their organisation. The *develop* and *implement* aspects can be to identify what elements are needed for a key management plan and work with others or alone to get these elements in place for a specified system that uses encryption. Examples could include SSL certificates for websites, SSH keys for server access or using Bitlocker to encrypt hard drives and managing the keys within Active Directory.

OPTION 2: RISK ANALYST

Competency Standard	Minimum, expected, requirements for a pass	Comments on criteria
Make cyber security risk assessments	The apprentice should be able to: • Conduct a cyber-risk assessment against an externally (market) recognised cyber security standard using a recognised risk assessment methodology. • Identify threats relevant to a specific organisation and/or sector.	The scope of the risk assessment should be broader than the one carried out under 'React to threats, hazards, risks and intelligence' but one assessment could provide evidence for both competencies. The organisation and/or sector should be that of the employer or one of their customers or suppliers if risk assessing 3rd parties is part of the role.
Develop security policy and processes	The apprentice should be able to: • Develop an information security policy or process to address an identified risk. • Develop an information security policy within a defined scope to take account of a minimum of 1 law or regulation relevant to cyber security.	The law or regulation should be relevant to the employer and the apprentice should be able to demonstrate the policy or process has been adopted by employer/client or explain why it has not.
Provide audit and assurance	The apprentice should be able to take an active part in a security audit against a recognised cyber security standard, undertake a gap analysis and make recommendations for remediation.	The apprentice should be able to demonstrate how the audit and gap analysis recommendations comply with the security standard used.
Develop incident response and business continuity plans	The apprentice should be able to: • Develop an incident response plan for approval (within an organisations governance arrangements for incident response). • Develop a business continuity plan for approval (within an organisations governance arrangements for business continuity).	The incident response and business continuity plans don't need to be approved and in use in the organisation but do need to take the exiting governance arrangements into consideration. Where this is the case the apprentice could demonstrate how the plans fit with the current arrangements and explain why they have not been approved.
Improve the cyber security culture in an organisation	The apprentice should be able to: • Assess security culture using a recognised approach. • Design and implement a simple 'security awareness' campaign to address a specific aspect of a security culture.	This is based around the existing culture within an organisation. The apprentice will know what that culture is and will be demonstrating a response to an identified problem. The assessment could involve using performance metrics that may be used, or in the form of a questionnaire, tests of employees' knowledge and understanding, reviews of incidents etc.