ST0865 Level 3 Cyber Security Technician Assessment Plan

Introduction

This Apprenticeship Assessment Plan (AAP) sets out the requirements for the assessment of the level 3 cyber security technician apprenticeship. It should be read in conjunction with the General Requirements for Apprenticeship Assessment. Where there is conflict between this AAP and the General Requirements, this AAP takes precedence. Assessment organisations must also comply with the relevant regulatory framework for apprenticeship assessment.

It is important that the assessment of apprentices is proportionate, valid, and provides reliable evidence of an apprentice's attainment of the relevant knowledge and skills. As such, assessment organisations must design assessments to ensure:

- employers have confidence that the apprentice has reached the expected performance standard
- apprentices are sufficiently secure in their knowledge and skills, so that they could demonstrate their competence in different contexts (for example, a different workplace)

Assessment Outcomes

The assessment outcomes group and summarise the knowledge and skills that must be demonstrated in assessments. All assessment outcomes must be assessed.

Knowledge and skills statements in **bold** are mandatory and must be assessed in every version of the assessment that is made available.

Assessment Outcome	Mapping
AO1: Information security governance, policy and culture Applies organisational information security governance principles, interprets relevant legislation and standards, and contributes to the review of information security policies. Promotes and supports a positive security culture by developing information security awareness resources.	**K1**, **K2***, **K3**, **K4***, **K5, K7**, **K20***, K23, K24*, K25, K28 **S1, S3,** S4, S18*, **S22**

Assessment Outcome	Mapping
AO2: Technical security controls and infrastructure operations Implements and maintains technical security controls across digital systems, networks, devices and cloud environments. Uses established procedures to configure, update and operate security technologies, manage access rights, and maintain accurate inventories of information assets.	**K8**, K9*, **K11**, **K12**, K13 **S2, S6, S9,** S10*
AO3: Security monitoring, detection and incident response support Monitors digital environments to identify information security events, categorises and escalates incidents, and documents event information while preserving evidence. Applies threat identification techniques and supports incident response processes in line with organisational procedures.	**K10***, K16, **K17,** K18, **K19*** **S7*, S8,** S13*, **S16***
AO4: Vulnerability, threat and risk assessment Conducts vulnerability assessments to an agreed scope, evaluates assessment results, and gathers threat intelligence from verified sources. Identifies and categorises threats, vulnerabilities and risks, and contributes to digital information risk assessments and business impact analysis.	**K14**, **K15***, **K27** S11, **S12*, S14*** S15
AO5: Compliance, audit and assurance activities Performs cyber security compliance checks, interprets audit requirements, and collates evidence from logs, reports and other data sources. Supports internal and external audit processes by documenting findings in appropriate formats and applying principles of information assurance.	**K6**, K21* S19, S20
AO6: Communication, collaboration and professional practice Communicates appropriately with technical and non-technical stakeholders, contributes to multidisciplinary team activities, and supports escalations. Maintains up-to-date knowledge of cyber security developments, applies ethical data practices, and recognises the wider organisational and societal context of their role.	**K22**, **K26,** K29, **K30** S5, **S17*, S21**

(*) Knowledge and skills statements which offer opportunities to develop functional English and maths are identified with an asterisk.

Assessment requirements

Assessment organisations must set apprenticeship assessments. Assessment organisations should consider how technology and digital tools can support innovation and efficiency.

Assessment organisations must design apprenticeship assessments to include at least one simulation.

Any additional assessment(s) must be selected from the following list of methods to ensure the assessment outcomes are met in full:

- **professional discussion**
- **question and answer**
- **portfolio**
- **presentation**
- **additional simulation**

Apprentices may be assessed at any appropriate point during their apprenticeship programme.

Assessments may be designed to allow a centre or training provider to mark assessments. The assessment organisation is responsible for ensuring all assessments are sufficiently reliable and valid, and for the accuracy of any centre or training provider marking.

Performance descriptors

Performance descriptors describe the level of performance required to achieve a pass or distinction grade. Assessment organisations must design assessments that align with these descriptions.

Performance Category	Pass	Distinction
Applied Knowledge	Demonstrates sound application of cyber security knowledge, facts, procedures and ideas across routine and non-routine tasks in familiar but sometimes complex work contexts, showing understanding within set parameters and	Demonstrates thorough understanding of cyber security knowledge, facts, procedures and ideas across routine and non-routine tasks**,** applying them proactively and resourcefully with minimal oversight**,** showing refined judgement

	with a degree of autonomy.	when navigating nuanced issues.
Applied Skills	Identifies and applies appropriate cyber security skills, methods and procedures to complete routine and non-routine tasks in familiar but sometimes complex contexts, working within set parameters and with a degree of autonomy and effectiveness.	Selects and integrates appropriate cyber security skills, methods and procedures to address routine and non-routine tasks, working proactively and resourcefully with minimal oversight, and demonstrating refined judgement when responding to nuanced issues.
Regulatory and Procedural Awareness	Demonstrates sound application of relevant cyber security legislation, regulations, organisational procedures and standards across routine and non-routine tasks, operating within set parameters and showing a degree of autonomy in familiar but sometimes complex contexts.	Demonstrates thorough understanding of relevant cyber security legislation, regulations, organisational procedures and standards, applying them proactively and resourcefully with minimal oversight, and showing refined judgement when navigating nuanced issues.
Communication and Collaboration	Communicates and collaborates effectively in cyber security team environments, adapting language to different audiences and contributing to routine and non-routine tasks with a degree of autonomy, showing sound application of communication practices in familiar but sometimes complex contexts.	Communicates and collaborates with refined judgement, adapting confidently to varied audiences and selecting and integrating communication approaches to support routine and non-routine tasks, working proactively and resourcefully with minimal oversight in nuanced team environments.
Information Use and Decision Making	Accurately interprets and evaluates relevant cyber security information from a variety of sources, making decisions that show sound application of knowledge and methods across	Confidently interprets and evaluates relevant cyber security information from a variety of sources, making decisions that demonstrate thorough understanding, refined

	routine and non-routine tasks, with some depth of insight and adaptability in familiar but sometimes complex contexts.	judgement, and the ability to navigate nuanced issues proactively and resourcefully with minimal oversight**.**
Responsibility and Autonomy	Takes responsibility for completing cyber security tasks within set parameters, working with a degree of autonomy and effectiveness across routine and non-routine tasks in familiar but sometimes complex contexts.	Takes responsibility for completing cyber security tasks proactively and resourcefully with minimal oversight**,** demonstrating refined judgement and confidently navigating nuanced issues across routine and non-routine tasks**.**

Professional recognition

This apprenticeship aligns with the professional body recognition detailed in the occupational standard.

Please contact the relevant professional body for further information.