# ST1021 Level 4 Cyber security technologist Assessment Plan

## Introduction

This Apprenticeship Assessment Plan (AAP) sets out the requirements for the assessment of the Level 4 cyber security technologist 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.

Assessment organisations must ensure all the core assessment outcomes and the assessment outcomes for one of the following options are assessed for each apprentice:

- Option 1: Cyber security engineer
- Option 2: Cyber risk analyst
- Option 3: Cyber security defend and respond

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

| Core Assessment Outcome | Mapping |
|---|---|
| **AO1: Threat, Vulnerability and Risk Identification**<br>Discover and report threats, vulnerabilities and hazards to inform risk assessment and selection of security controls. | **K3, K4, K11,** K13<br><br>S1, S2, S9, S17, S27 |

| | |
|---|---|
| **AO2: Cyber Security Technology Implementation**<br>Configure, deploy and use computer, digital network and cyber security technology. | **K1**, K2, K12, **K16**<br>**S8** |
| **AO3: Secure Automation and Digital Solutions**<br>Develop instructions (code, script or prompts) that cause a computer or other digital systems to deliver intended outcomes, and validate the outcomes. | K17<br>**S13** |
| **AO4: Cyber Security Operations Management**<br>Demonstrate management of cyber security operations processes in accordance with organisational policies, standards and business requirements. | K6, **K8**, **K9**, K15<br>**S7** |
| **AO5: Cyber Security Exercising and Preparedness**<br>Participate in a cyber exercise or simulation (technical or non-technical) to test and rehearse cyber security and incident response and learn lessons. | **S30** |
| **AO6: Professional Cyber Security Practice**<br>Actively maintain up to date knowledge and application of cyber security threats, vulnerabilities, technology and evolving recognised professional practice. | K5<br>**S3**, S9 |
| **Option 1: Cyber Security Engineer** | **Mapping** |
| **AO7: Secure Solution Design and Assurance**<br>Analyse security requirements including applicable laws & regulations to make a reasoned security case and design and implement a secure solution in accordance with the security case. | **K10**<br>S5, **S6**, S10, S11, **S12**, S14 |
| **AO8: Security Monitoring, Detection and Protection**<br>Select and configure monitoring, detection and prevention tools, techniques and processes to mitigate impact of cyber security incidents in an organisational context. | **K7**<br>**S15**, **S25**, **S28** |
| **Option 2: Cyber Risk Analyst** | **Mapping** |
| **AO9: Cyber Risk Assessment and Treatment**<br>Conduct a cyber risk assessment taking account of security, legal & regulatory requirements and acceptable consequences in an organisational context with reasoned recommendations. | **K10**, K14<br>**S4**, S5, **S6**, **S16**, S20, S22 |

| | |
|---|---|
| **AO10: Security Culture and Awareness**<br>Design and implement a security awareness campaign or organisation security policy to address a security priority and collect feedback to assess impact. | **S18**, S19, S23, S24 |
| **Option 3: Cyber Security Defend and Respond** | **Mapping** |
| **AO11: Security Analysis and Decision Making**<br>Demonstrate ability to critically assess a variety of sources to determine a justified course of action in accordance with organisational policy and procedures. | **K7**<br>S21, **S25**, **S26**, S29 |
| **AO12: Security Monitoring, Detection and Protection**<br>Select and configure monitoring, detection and prevention tools, techniques and processes to mitigate impact of cyber security incidents in an organisational context. | **S15**, **S28** |

**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 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:

- **Project**
- **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** | Applies sound application of theoretical and technical cyber security knowledge in a broad range of complex technical work activities, performed in a variety of contexts. Applies sound reasoning to address varied and occasionally complex problems which are normally fairly well-defined, producing generally effective outcomes within the cyber security context. | Applies precise application of theoretical and technical cyber security knowledge in a broad range of complex technical work activities, performed in a variety of contexts. Solves to improve outcomes when addressing complex and non-routine problems which are normally fairly well-defined, consistently producing high-quality outputs within the cyber security context. |
| **Applied Skills** | Selects and applies suitable cognitive and practical skills in a broad range of technical work activities, performed in a variety of contexts, to solve varied and occasionally complex cyber security problems which are normally fairly well-defined. Selects and applies consistently appropriate methods, adapting to meet requirements and achieving outcomes that meet organisational expectations. | Adapts and applies with flexibility and operational fluency suitable cognitive and practical skills in a broad range of technical work activities, performed in a variety of contexts, to solve complex and non-routine cyber security problems which are normally fairly well-defined. Methods are optimised for quality, efficiency and improved outcomes. |
| **Regulatory and Procedural Awareness** | Applies cyber security legislation, regulation and organisational security procedures relevant to the cyber security context with sound judgment**,** adapting | Applies evaluation of cyber security legislation, regulation and organisational security procedures relevant to the cyber security context with |

| | | |
|---|---|---|
| | appropriately to varied and occasionally complex situations within broad but generally well-defined parameters. | insight and complexity, identifying implications and making informed decisions that improve outcomes in varied and occasionally complex situations. |
| **Communication and Collaboration** | Communicates clearly and collaborates effectively with colleagues and stakeholders, adapting, to meet different needs or contexts. Contributes effectively to responsive service delivery and team working within cyber security activities. | Communicates confidently with colleagues and stakeholders, tailoring, effectively for different needs or contexts. Actively supports improved collaboration and service delivery outcomes through effective team working within cyber security activities. |
| **Information Use and Decision Making** | Analyses and interprets information from a range of sources relevant to the cyber security context to determine well supported conclusions with sound reasoning and make informed decisions for courses of action, demonstrating awareness of the broader occupational context. | Applies evaluation of information from a range of sources relevant to the cyber security context to reach informed conclusions, providing insightful justification for decisions that improve outcomes and demonstrating awareness of wider implications within the occupational area. |
| **Responsibility and Autonomy** | Takes responsibility for actions and decisions, including where relevant managing own work and coordination of others within the cyber security context. Operates within broad but generally well-defined parameters, applying awareness of risks and priorities when determining courses of action. | Proactively takes responsibility for actions and decisions, with confident autonomy and sound judgment within the cyber security context. Manages own work and the coordination of others, independently determining priorities, risks and appropriate courses of action within broad but generally well-defined parameters. |