BCS Digital Industries Apprenticeship

Standard Specific Guidance for Training Providers

Level 4 Cyber Security Technologist Apprenticeship

Version 5.0
April 2019

Change History

Any changes made to the project shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number and Date	Changes Made
V1.0 June 2017	Document created
V1.1 September 2017	Removed SFIAplus codes
V2.0 November 2017	Updated competencies
V3.0 January 2018	Update to technical competencies, knowledge standards and work activities.
V4.0 January 2019	Document updated with revised SFIAplus codes and new format.
V5.0 April 2019	Updates to proficiencies Business Skills, Complexity, Autonomy and Influence throughout the document.

Contents

Purpose of this Document

The purpose of this document is to provide useful information and suggested supporting documentation specific to the cyber security technologist apprenticeship. It should be read in conjunction with the BCS General Guidance for Apprentices, Employers and Training Providers document and is designed to give training providers some tools to help them build their own programme from training plan through to end-point assessment.

This guide will provide:

- supporting information around how to help the cyber security technologist apprentice to meet and go beyond the standard;
- a number of useful documents to support the training provider in meeting their responsibilities in managing the apprenticeship from training plan through to the end-point assessment;
- evidence checklists to help the training provider support the apprentice in completing their summative portfolio;
- a template for completing the employer reference.

Introduction

The BCS Level 4 Cyber Security Technologist Apprenticeship is one of the suite of Digital Industries Apprenticeships that have been designed by the industry to address skills shortages and meet the ever-changing needs of UK employers.

The General Guidance for Apprentices, Employers and Training Providers provides the broad view on how to run an apprenticeship programme to the BCS Digital Industries Standard. The collection of tables and templates contained within this document has been designed to give training providers the tools to build their programme and to assist them in helping apprentices and employers towards the successful completion of each element of the end-point assessment.

The areas where a training provider should be involved in ensuring a successful outcome to the apprenticeship are:

- mapping and assessing work against the standard;
- advising the employer and the apprentice on which knowledge modules, vendor or professional certificates and other relevant training and activities are most appropriate for their requirements, and agree a suitable training plan;
- assisting the apprentice with applying knowledge in the workplace;
- acting as an advisor to the apprentice and the employer to ensure the programme remains on track and any concerns are addressed;
- helping the apprentice to select evidence for their summative portfolio;
- supporting the apprentice through the synoptic project;
- confirming the apprentice's readiness for the end-point assessment.

The following series of checklists can be used by the training provider to help manage the process through to completion. Training providers may substitute their own processes and documentation as they see fit in order to effectively manage their key areas of responsibility as set out above.

The Cyber Security Technologist Apprentice

The primary roles of a cyber security technologist are to:

- apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations, systems and people;
- achieve required security outcomes in a legal and regulatory context in all parts of the economy;
- develop and apply practical knowledge of information security to deliver solutions that fulfil an organisation's requirements.

Job titles may be different across different organisations so the role may also be referred to as cyber operations manager, security architect, penetration tester, security analyst, risk analyst, intelligence researcher, security sales engineer, cyber security specialist, information security analyst, governance and compliance analyst, information security assurance and threat analyst, forensics and incident response analyst, security engineer, information security auditor, security administrator or information security officer.

Business Proficiencies

The proficiencies that should be demonstrated by an apprentice cyber security technologist are listed below.

Business skills

- The apprentice can demonstrate an analytical and systematic approach to issue resolution.
- The apprentice takes the initiative in identifying and negotiating appropriate personal development opportunities.
- The apprentice can demonstrate effective communication skills.
- The apprentice can contribute fully to the work of teams.
- The apprentice plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures.
- The apprentice can appreciate the wider business context, and how their role relates to other roles and to the business of the employer or client.

Complexity

- The apprentice can perform a range of work, sometimes complex and non-routine, in a variety of environments.
- The apprentice can apply a methodical approach to issue definition and resolution.
- The apprentice undertakes all work in accordance with agreed safety, technical and quality standards, using appropriate methods and tools.

Autonomy

- The apprentice can operate under general direction.
- The apprentice uses discretion in identifying and responding to complex issues and assignments.

- The apprentice can receive specific instructions and has work reviewed at frequent milestones.
- The apprentice can determine when issues should be escalated to a higher level.

Influence

- The apprentice interacts with and influences colleagues.
- The apprentice has working level contact with customers, suppliers and partners.
- The apprentice may supervise others or make decisions which impact the work assigned to individuals or phases of projects.
- The apprentice makes decisions which influence the success of projects and team objectives.

Knowledge standards, technical competence and behaviour and relationship standards

Tables 1, 2 and 3 contain details of the topics that the training provider may decide to cover in their development plans and scheduled work activities in order to stretch the apprentice.

Table 1 – Cyber Security Technologist – Knowledge Standards

The knowledge standards define learning that must take place during the apprenticeship, **both through the activities and the apprentice's own independent learning**. The additional learning outcomes detailed in the table show how a training provider can stretch the apprentice's learning beyond the requirement as set out in the occupational brief. However, it is important to remember that stretching the apprentice in this way will only have a bearing on their final grading if the impact is demonstrated through their competence in the end point assessment. These knowledge standards, therefore, show the additional learning that may support the apprentice in improving their overall competence. Technical knowledge and understanding is assessed throughout the apprenticeship through a combination of Ofqual regulated knowledge modules and specified vendor and professional qualifications. These must be passed before the end point assessment can take place.

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
Understands the basics of cyber security.	The apprentice will be able to explain; Why cyber security matters • Explain why information and cyber security is important to business and society. Basic security theory • Explain basic concepts: security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard. This should illustrate an understanding of what fundamentally security is and the basic concepts of risk, threat, vulnerability and hazard. • Explain how the concepts of threat, hazard and vulnerability relate to each other and lead to risk. Describe in simple terms what risk is and how risks are usually characterised (likelihood and impact) and illustrate by use of at least one commonly used tool (e.g. a risk register). • Understand the inherent asymmetric nature of cyber security threats. • Describe and characterise (in terms of capability, opportunity and motive) examples of threats and also describe some typical hazards that may concern an organisation. Recognise that there are different types or classes of threat	<u>Why Cyber Security Matters</u> Describe and explain the evaluation of information assets and the criticality to a business. Describe and explain how cyber security can have a direct impact on the reputation and continuing success of a business. Describe and explain how the cyber security of businesses contributes to the overall economy and security of the society in which it operates. <u>Basic Security Theory</u> Recall and explain key terminology. • Security • Identity • Authentication • Non-repudiation • Confidentiality • Integrity • Availability • Threat • Vulnerability • Risk and hazard Describe what security is, fundamentally, by explaining: • How the concepts of threat, hazard and

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	and threat actor and that these may be profiled. Relate these descriptions to example security objectives. • Understand how an organisation balances business drivers with the outcome and recommendations of a cyber security risk assessment, taking account the wider business risk context Security assurance • Assurance concepts: explain the difference between 'trusted' and 'trustworthy' and explain what assurance is for in security. Describe the main approaches to assurance (intrinsic, extrinsic, design and implementation, operational policy and process) and give examples of how these might be applied at different stages in the lifecycle of a system. • Assurance in practice (reference the concepts): explain what penetration testing ('ethical hacking') is and how it contributes to assurance. Describe at least one current system of extrinsic assurance (e.g. security testing, supply chain assurance, Common Criteria) explaining the benefits and limitations. Describe at least two ways an organisation can provide intrinsic	vulnerability relate to each other and lead to risk. • The inherent asymmetric nature of cyber security threats. Describe and explain: • What risk is • How risks are usually quantified (by likelihood and relative impact) • The use of at least one commonly used tool for risk management; for example, but not limited to, a risk register. Describe typical threats, threat actors and hazards in terms of capability, opportunity and motive using examples that may concern an organisation: • Profiling techniques • Relating these threat descriptions to example security objectives Describe and explain how an organisation balances business drivers and costs with the outcome and recommendations of a cyber security risk assessment. Apprentices will also consider the wider business risk context using, as an example: • a business impact assessment (BIA).

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement

	assurance.
	
	Applying basic security concepts to develop security requirements (to help build a security case)
	• Derive and justify security objectives. Describe how these might apply to information and infrastructure assets in at least two different and representative business scenarios, including a reasoned justification (taking account of the value of the assets) of the different importance and relative priorities in the different scenarios. Explain and illustrate by example how this analysis leads to an expression of security objectives or requirements.
	
	Security concepts applied to ICT ('cyber') infrastructure
	• Describe some common vulnerabilities in computer networks and systems (for example, non-secure coding and unprotected networks)
	• Describe the fundamental building blocks (e.g. routers, switches, hubs, storage, transmission) and typical architectures (e.g. server/client, hub/spoke, non-virtual/virtual) of computers, networks and the Internet.
		<u>Security Assurance</u>
		
		Recall, describe and explain security assurance concepts and how these might be applied at different stages in the lifecycle of a system:
		
		• The difference between 'trusted' and 'trustworthy'
		• The purpose of security assurance
		• The main approaches to:
		  ○ Assurance
		  ○ Intrinsic and extrinsic
		  ○ Design and implementation
		  ○ Operational policy and process
		
		Describe and explain the way security assurance works in practice regarding the concepts.
		
		Describe and explain what penetration testing is and how it contributes to security assurance; for example, 'ethical hacking'. Apprentices will also show an understanding of the differences between internal and external penetration testing.
		
		Describe at least one current system of extrinsic assurance, explaining the benefits and limitations:
		
		• Security testing
		• Supply chain assurance
		• Common criteria
		
		Describe at least two ways an organisation can provide

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	Attack techniques and common sources of threat • Describe the main different types of common attack techniques (for example, phishing, social engineering, malware, network interception, blended techniques e.g. 'advanced persistent threat', denial of service, theft). Explain the main features of how they work and suggest where they may be effective. • Describe the role of human behaviour in cyber security. Explain what 'the insider threat' is. Explain what 'cyber security culture' in an organisation is, describe some features that may characterise it and explain how it may contribute to security risk. • Explain how an attack technique combines with motive and opportunity to become a threat. Explain how attack techniques are developed and why they are continuously changing. • Describe typical hazards and how these may achieve the same outcome as an attack (e.g. flood, fire). Cyber defence • Describe ways to defend against the main attack techniques, including	intrinsic assurance. <u>Applying Basic Security Concepts to Develop Security Requirements</u> Explain how to develop and justify security objectives for a proposed business solution. Describe how security objectives might be used to define information and infrastructure assets in representative business scenarios. Explain how security objectives might be justified, taking account of the value of the assets, by understanding the importance and relative priorities in the different scenarios. Explain how analysis of security objectives leads to an expression of security requirements and how this assists both with the building of a security case and in the development of the new system. <u>Security Concepts Applied to ICT Cyber</u> Show an understanding of common vulnerabilities in computer networks and systems. This may include, non-secure coding and unprotected networks. Describe the fundamental building blocks of: • Infrastructure elements:

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	consideration of 'deter', 'protect', 'detect' and 'react' and an 'attack chain'. Legal, standards, regulations and ethical standards relevant to cyber security • Describe the cyber security standards and regulations and their consequences for at least two sectors (e.g. Government, finance, petrochemical/process control), comparing and contrasting the differences. • Appreciate the role of criminal law, contract law and other sources of regulation. • Explain the benefits and costs and the main motives for uptake of significant security standards such as Common Criteria, PCI-DSS, FIPS-140-2, CESG Assisted products (CAPS). • Describe the key features of the main English laws that are relevant to cyber security issues (including legal requirements that affect individuals and organisations), for example the Computer Misuse Act, Data Protection Act, Human Rights Act. • Describe the implications of international laws and regulations that	○ Firewalls ○ Routers ○ Switches ○ Hubs ○ Storage ○ Transmission. • Typical architectures of computers, networks and the Internet: ○ Server/ client ○ Hub/spoke ○ Non-virtual/ virtual. <u>Attack Techniques and Common Sources of Threat</u> Describe and explain the main types of attack techniques. For each type of attack, apprentices should illustrate the main features of how they work and suggest where and when they may be effective. • Current attack types may include: ○ Phishing ○ Social engineering ○ Malware ○ Network interception • Blended techniques may include: ○ Advanced persistent threat (APT) ○ Denial of service (DoS and DDoS) ○ Information theft and ransomware.

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	affect organisations, systems and users in the UK, movement of data and equipment across international borders and between jurisdictions (e.g. Digital Millennium Act, ITAR, Safe Harbour). • Describe the legal responsibilities of system users and how these are communicated effectively. • Describe by reference to at least one generally recognised and relevant professional body the ethical responsibilities of a cyber-security professional. Keeping up with the threat landscape • Describe and know how to apply at relevant techniques for horizon scanning and be able to identify at least three external sources of horizon scanning (e.g. market trend reports, academic research papers, professional journals, hacker conferences, government sponsored sources, e.g. CISP) and recognise the value of using a diversity of sources. Illustrate with some current examples relevant to cyber security. Describe and know how to apply at least one technique to identify trends in research. Illustrate with an example.	Describe the role of human behaviour in cyber security, including an ability to: • Explain the term 'insider threat' • Explain an organisation's 'cyber security culture' and describe some features that may characterise it. Apprentices should also show an understanding of how this cyber security culture may contribute to security risk. Explain how an attack technique combines with motive and opportunity to become a threat. Apprentices should also illustrate how attack techniques are developed and why they are continuously changing. Describe typical hazards and how these may achieve the same outcome as an attack. For example, flood and fire. <u>Cyber Defence</u> Describe ways to defend against attack techniques by considering the different ways in which controls may be used; including: • Deter, protect, detect and react • Preventative, directive, detective and corrective • Physical, procedural (people) and technical • An attack chain

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	Future trends • Describe the significance of some identified trends in cyber security and understand the value and risk of this analysis.	<u>Legal, Regulatory, Information Security and Ethical Standards Relevant to Cyber Security</u> Describe the appropriate and applicable cyber security standards, regulations and their consequences for at least two sectors, comparing their differences: • Government • Public sector • Charitable • Finance • Petrochemical / process control. Describe and explain the role of criminal law, contract law and other related sources of legal and regulatory control. Describe and explain the benefits, costs and main motives for the uptake of significant security standards; including: • Common Criteria • PCI-DSS • FIPS-140-2 • CESG Assisted products (CAPS) • COBIT Describe and explain the main features and implications of laws and regulations that affect organisations, systems and users in the UK: • The main UK laws that are relevant to cyber security issues, including legal requirements that

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		affect individuals and organisations. Examples could include: ○ The Computer Misuse Act ○ The Data Protection Act (DPA) ○ The Human Rights Act • The international laws and regulations that affect organisations, systems and users in the UK covering the movement of data and equipment across international borders and between jurisdictions; including: ○ The Digital Millennium Act ○ International Traffic in Arms Regulations (ITAR) ○ Harbour (Safe Harbour) ○ The Patriot Act ○ General Data Protection Regulations (GDPR) ○ The Network and Information Security Directive (NIS) The legal responsibilities of system users and how these may be communicated effectively. Describe and explain the ethical responsibilities of a cyber-security professional, by reference to at least one generally recognised and relevant professional body influential in the UK. <u>Keeping Up with The Threat Landscape</u> Describe and know how to apply relevant techniques for

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement

		horizon scanning and can:
		• Recall, discover and explain the relative merits of at least three external sources of horizon scanning. These may include:
		  ○ Market trend reports
		  ○ Academic research papers
		  ○ Professional journals
		  ○ Hacker conferences
		  ○ Online
		  ○ Government sponsored sources; including: The National Cyber Security Centre (NCSC), CiSP and CertUK
		• Describe and explain the value of using a diversity of sources
		• Explain the horizon scanning technique, using current examples from sources relevant to cyber security in the UK
		• Determine the reliability and trustworthiness of different sources.
		Describe and explain the application of at least one technique to identify trends in research and illustrate with an example.
		
		<u>Future Trends</u>
		Describe and explain the significance of some identified

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		trends in cyber security. Explain the value and risk of this analysis.
Understands the basics of networks.	The apprentice will be able to: • Explain what is meant by data and protocol and how they relate to each other. Describe an example data format and a simple protocol in current use (using protocol diagrams). • Describe example failure modes in protocols, for example reasons why a protocol may 'hang' and the effect on a protocol of data communication errors, • Describe at least one approach to error control in a network. Describe the main features of network protocols in widespread use on the Internet, their purpose and relationship to each other in a layered model (e.g. TCP/IP), including the physical and data link layer. (e.g. HTTPS, HTTP, SMTP, SNMP, TCP, IP, etc.). • Describe the main routing protocols in current use in computer networks and explain the differences between static and dynamic routing protocols and the pros and cons of each in different circumstances. • Explain some of the main factors that affect network performance (e.g. the	<u>Network Data and Protocols.</u> Describe data formats and protocols in current use. Explain features of network protocols in widespread use on the internet. Including: • HTTPS; • HTTP; • SMTP; • SNMP; • TCP; • UDP; • IP. Identify network failure modes and reasons why networks 'hang'. Describe approaches to error control in a network. <u>Layered Network Models.</u> Explain features of the following layered network models: • TCP/IP Reference Model; • OSI 7 Layer Model. Compare the differences between the following physical

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	relationship between bandwidth, number of users, nature of traffic, contention) and propose ways to improve performance (e.g. application of traffic shaping, changes to architecture to avoid bottlenecks, network policy that prohibits streaming protocols).	layer categories and datalink layer protocols: • Physical Layers (including, but not limited to: wireless, fibre, wired); • Data Link Layer (including, but not limited to: Ethernet [802.3], Wireless LAN[802.11], Bluetooth). <u>Network Routing Protocols.</u> Describe current network routing protocols in use, including: • RIP/RIP2; • RIP-NG; • OSPF; • OSPFv2; • OSPFv3. Compare the differences between static and dynamic routing. <u>Network Performance.</u> Demonstrate the relationship between factors that affect network performance, including: • bandwidth; • number of users; • nature; • contention.

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		Explain methods of improving network performance, such as, traffic shaping and architecture.
Understands how to build a security case.	The apprentice will be able to: • Describe what good practice in design is and how this may contribute to security. • Describe common security architectures that incorporate security hardware and software components. Be aware of sources of reputable security architectural patterns and guidance (e.g. vendor or government). • Understand how to develop a 'security case'. (A security case, sometimes also called a `security target' describes the context, security objectives, threats, and for every identified attack technique identify a mitigation/security controls – technical, implementation or policy/process, recognizing that threats evolve and threats also respond to a security design).	<u>IT Security Design Principles.</u> Demonstrate the importance of keeping IT systems simple, whilst meeting business and security needs. Describe the application and features of core IT security design principles, including: • least privilege; • economy of mechanism; • defence in depth (complete mediation); • human factors – psychological acceptability; • fail-safe defaults; • open design; • separation of privileges; • least common mechanism. Explain the following features of the Trustworthy Software Initiative(TSI): • safety; • reliability; • availability; • resilience; • security.

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		Compare TSI and IT security design principles and explain their commonalities. <u>Common Security.</u> Demonstrate the difference between enterprise architecture and security architecture, and explain where their physical and logical boundaries may exist. Compare features of common security architectures, including: • SABSA; • Zachman Framework; • TOGAF; • CISCO and the NIST Cyber Security Framework. Relate how national bodies such as CESG, FIPS, NIST and GCHQ provide guidance and information to public and private sector organisations in the following areas: • IT security policies; • IT security architectural patterns / frameworks; • white papers; • national strategies on cyber security. <u>Common Criteria Protection Profile.</u> Explain the purpose and features of the Common Criteria evaluation model:

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		• Common criteria – their application and uses; • Target of Evaluation (TOE); • Protection Profile; • security target; • EALs; • the process of specification, implementation and evaluation for certified products and systems Describe how Common Criteria may be used to feed into a security case. <u>Security Case.</u> Produce a security case for a known system: • a clear definition of the objectives of the case: who, what, where, why and when; • threats that are likely to exist against the target system; • known attack profiles likely to be used by malicious individuals; • risks to the system, measured in probabilities (very likely, likely and unlikely); • potential impact (major, moderate, minor); • Potential severity (high, medium, low); • physical protection measures that maybe required: • CCTV / alarms; • backups;

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		• cabinets. Considering the security case, interpret what security measures should apply: Technical protection measures using hardware devices: • firewalls; • routers; • SIEM. Software components: • access rights; • anti-virus; • scanners. Implementation strategies for a proposed solution: • constraints; • dependencies; • cost benefit analysis. IT security policies that may be needed as part of the security case, including: backups and data protection. Where applicable, complete a test plan to include descriptors and expected results. Considering the security case:

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement

		• applicable processes that may need to be implemented by personnel or systems;
		• overview of legal responsibilities, where applicable;
		• staff training that maybe required for the new measures;
		• future proofing.
		• alternative solutions to the case for due consideration:
		  ○ OTS solutions;
		  ○ third-party contracts;
		  ○ complete software solutions.
		
		Describe (using software applications, hardware components and examples), how threats evolve over time to respond to system security hardening.

Understands how cyber security technology components are typically deployed in networks and systems to provide security functionality.	The apprentice will be able to: • Describe common types of security hardware and software which are used to protect systems (e.g. firewalls, encryption for data at rest, encryption for communication, IDS, IPS, IDAM tools, AV, web proxy, application firewalls, cross domain components, HSM, TPM, UTM) and explain how each may be used to deliver risk mitigation or implement a security case, understanding the benefits/limitations, and taking into	<u>Host-based Security.</u> Describe computer and data authentication methods in current use. Describe methods employed to protect and secure data held on the host: • types of authentication; • access control; • physical security; • TCP ports; • disk encryption; • checksums.

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	account the implicit assurance (including supplier assurance and considering the benefits and risks of open source options) of the component, describing any residual risks.	Explain the importance of and the methods employed to keep the software environment healthy and up to date: • zero day attacks; • operating system and application updates; • antivirus updates. Describe the responsibilities of the user for PC protection, in keeping their PC and its data secure from threats: • social engineering; • software updates; • password management; • Internet etiquette. <u>Network-based Security.</u> Describe the hardware components available for network protection and their purpose and demonstrate the ability to select the appropriate system for a given task: • firewalls and DPI; • application proxies; • IDSvs. IPS; • RADIUS; • AAA. Describe the policy based methods available for network

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		protection and explain their purpose: • QoS; • cross-domain components; • DMZ; • gateways; • routing; • traffic prioritisation; • anomaly and misuse detection Describe methods available for the protection of data whist in transit and demonstrate the ability to select from a range of current technologies and appropriate methods for the protection of data as it crosses arbitrary networks. Indicative areas of study are secure Internet transaction technologies: • IPSec • TLS • SSH • negotiation; • cryptography; • key management. Describe the responsibilities of network administrators and approaches available for the management of security in the network. Apprentices should also explain the necessity for network and server configuration and maintenance, as

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		well as available methods: • network segregation; • security issues for common client and server configuration; • performance management; • staff training; • file and user permissions; • password management. <u>Application of Security for Software and Data.</u> Describe frameworks and processes available for secure application development and apply appropriate security processes to the software development lifecycle: • OWASP Top 10 awareness for web application development • Common Weakness Enumeration guideline awareness for general software development • National Cyber Security Centre (NCSC) guidelines • Secure SDLC Describe IDAM Tools and systems available for application and data protection, and how these can be applied to manage application security: • identity management systems and protocols; • tickets; • tokens;

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		• sessions; • multi factor authentication; • access control; • definitions (identity, authentication, authorisation, Bell-LaPadula model). Describe application firewalls and reverse proxies and demonstrate the ability to select from a range of current technologies or appropriate tools to enhance the protection of data as it is captured and returned by applications: • application sensors; • application firewalls; • proxies and reverse proxies; • application level security logging and monitoring; • log configuration. Describe database security mechanisms, including the responsibility of encryption in protecting user data; show the necessity for securing data at rest and describe different ways this can be done using database applications: • field vs record based encryption; • SQL security; • backup security; • database access control. Management of Network Security and Risk in Networks.

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		Correctly apply risk mitigation techniques: • threat modelling (example STRIDE); • security controls (SANS Top 20, NIST 800-53, GPG 13). Apply security mechanisms as they relate to the CIA Triad; particularly, how to select security mechanisms to implement all three into a computer system: • confidentiality (select layers for encryption;) • integrity (validating the integrity of data transmissions); • availability (load balancing, proxies, anti-DDOS, WAF). Explain accreditation and assurance processes that relate to the application of security technology. Apprentices will be able to demonstrate the ability to apply supplier, software and component assurance and accreditation processes (first introduced in the Cyber Security Technologist, Knowledge Module 2): • penetration testing; • vulnerability assessment and threat intelligence; • ISMS and standards role in accreditation and supplier assurance (ISO27001, PCI DSS, common criteria, product assurance); • software code review (SAST, DAST, IAST,

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		reviews). Describe security technology solutions in terms of their benefits and limitations and explain strengths, weaknesses and applicability of security: • automation vs. manual validation of security; • open source vs. closed source solutions; • on premises vs. off premises solutions (cloud based, private, hybrid and public); • iterative vs. waterfall projects implication on security engineering.
Understands the basics of cryptography.	The apprentice will be able to: • Describe the main cryptographic techniques (e.g. symmetric, public key, secure hash, digital signing, block cipher etc.), how they are applied and to what end and their limitations (including study of some examples of badly applied or implemented cryptographic techniques). • Explain the significance of key management and the main features, benefits and limitations of symmetric and public key cryptosystems and the significance of entropy. • Describe the role of cryptographic techniques in a range of different systems (e.g. GSM, Chip & PIN, common hard disk encryption, TLS,	<u>Theory of Cryptographic Techniques.</u> Describe cryptographic techniques and state their limitations: • ciphertext vs. plaintext; • ciphers; • cryptographic techniques; • key length vs. Security; • hashing; • digital signatures; • attacks. Describe the main features of symmetric cryptosystems, PK cryptosystems and key exchange. Show where the various cryptographic techniques may be

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
	SSL, privacy enforcing technology) and the practical issues introducing such into service and updating them. • Appreciate that there are legal issues relevant to cryptography in particular when crossing national borders. Awareness of UK, EU and US export control of cryptography and the Wassenaar Arrangement and where to go to get advice.	employed to secure data and systems: • password verification; • digital signatures; • VPNs; • tunnelling; • encapsulating and carrier protocols; • IPsec. Show how poorly applied cryptography can become a threat vector: • ECB mode; • collision attacks; • algorithm problems; • key management problems; • random number generation problems. Explain the significance and role of entropy in cryptography and discuss security problems associated with entropy. <u>Deployment of Cryptography.</u> Explain the significance of key management as it relates to controls, lifecycle and governance. Describe the role of cryptography in a range of common public systems:

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		• mobile telecommunications; • secure card payments; • cyber applications; • video broadcasting; • private and home user considerations. Describe the role of cryptography as it applies to data on hard disks or in transit: • secure Internet transaction technologies; • data at rest; • open vs closed source. List some of the practical issues encountered in implementing cryptography: • performance considerations; • storage of keys; • security clearance of custodians; • historical consideration of broken cryptographic systems; • theoretical vs practical security; • Kerckhoff's principle. Explain the practical issues faced when updating cryptographic techniques: • vulnerability analysis; • intelligence sources;

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		• general understanding of validation processes; • patching process and testing. <u>Cryptography across Jurisdictions.</u> List the regulatory frameworks in place in different jurisdictions; • International Traffic in Arms Regulations; • DPA; • FoI; • the Combined Code; • Sarbanes–Oxley and their areas of governance; • RIPA 2000; • key escrow; • International Data Encryption Algorithm (IDEA). Describe some of the legal issues related to cryptography with respect to national borders. List a range of resources available to obtain advice concerning cryptography and security: • CAVP; • CVE lists; • open vs. closed reviews; • ISO; • OWASP; • SANS; • NIST;

Knowledge standard	Expected requirement	Suggested learning outcomes to meet the standard and stretch the apprentice to exceed the minimum requirement
		• NCSC.

Table 2 – Cyber Security Technologist – Technical Competency Standards

The competency standards have been defined to demonstrate that the knowledge learnt has been applied in real work tasks, activities and projects in a business environment.

Competencies are assessed throughout the apprenticeship through a combination of the employer reference, the synoptic project and a summative portfolio completed by apprentices from records of the work activities in which they have been involved.

The training provider should assist the employer to identify suitable work tasks, activities and projects within the scope of their normal business activities for the apprentice to practice what they have learnt and to demonstrate the competencies below.

The BCS Apprenticeship is mapped to an internationally recognised skills framework and to work activities in which a cyber security technologist apprentice would be involved.

The following table sets out these competencies and the expected requirements against the work activities that might be demonstrated at and beyond the minimum expectation. The format is explained below:

Competency standard	**Expected requirement**	**Work activities demonstrating the minimum expected level of competence**
This column contains the competency as it is listed in the apprenticeship standard.	*This column shows the expected requirements listed in the occupational brief for a successful outcome.*	*This column shows recognised work activities that demonstrate that the apprentice is meeting the expected requirement.* *The apprentice should be able to demonstrate all of these activities.*

The Cyber security technologist competency standard, requirements and activities demonstrating competence follow:

Competency standard	Expected requirement	Work activities demonstrating expected level of competence
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.	• Reviews network usage. Assesses the implications of any unacceptable usage and breaches of privileges or corporate policy. Recommends appropriate action
Developing and using 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).	• Conducts security control reviews in well defined areas. Assesses security of information and infrastructure components. Investigates and assesses risks of network attacks and recommends remedial action.

Competency standard	Expected requirement	Work activities demonstrating expected level of competence
Organisational context	The apprentice should be able to: • Identify and follow organisational policies and standards for information and cyber security. • Operate according to service level agreements or employer defined performance targets.	• Supports service level management in monitoring the impact of network problems on agreed service levels.
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.	• Uses new approaches, proposals and technologies to build a credible strategy, building on understanding of business needs, the existing IT capabilities and future requirements, marrying all relevant organisation objectives with achievable IT goals.
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.	• Produces outline system designs and specifications covering objectives, scope, features, facilities, management, reliability, resilience, security, constraints (such as performance, resources and cost), hardware, network and software environments, main system functions and information flows, traffic volumes, data load and implementation strategies, phasing of development, requirements not met, and alternatives considered.
Analysing 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 tradeoffs.	• Explains the purpose of and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls. (For example the key controls defined in IS27002). Communicates information assurance risks and requirements effectively to users of systems and networks.

Competency standard	Expected requirement	Work activities demonstrating expected level of competence
Structured and reasoned implementation of security in a network	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.	• Contributes to the development of solution architectures in specific business, infrastructure or functional areas, using appropriate tools and methods.

Criteria for demonstrating **Significantly** higher competencies.
Understands and applies a wide range of tools and methods.
Accurately and appropriately applies and effectively implements the right tools and methods in a variety of different situations.
Extensive and deep understanding of different tools and methods and how and why they can be applied in different contexts.
Deals confidently and capably with a high level of interrelated and interdependent factors in their work.

Table 3 – Generic Behaviour and Relationship Standards

The behaviour and relationship standards have been defined to demonstrate that the apprentice applies the good behaviours and interpersonal skills that are needed in a business environment. Behaviours and business relationship skills are assessed throughout the apprenticeship through a combination of the employer reference, the synoptic project and a summative portfolio, which is completed by apprentices from records of the work activities in which they have been involved. The training provider could assist the apprentice by offering some additional soft skills training over and above their apprenticeship. The apprenticeship standard sets out the attributes required within the occupation brief, which can be accessed via the Apprenticeship section of www.bcs.org.

Behaviour and relationship standard	Expected requirement
Apprentices can demonstrate the full range of skills, knowledge and behaviours required to fulfil their job role.	Knows what skills, knowledge and behaviours are needed to do the job well. Are aware of their own strengths in the job role, and any areas for improvement. Appreciate who else is important, for them to do their job and fulfil the role effectively (e.g. colleagues, managers, other stakeholders). Are aware of potential risks in the job role (e.g. security, privacy, regulatory). Use personal attributes effectively in the role, e.g. entrepreneurship. Understand how the job fits into the organisation as a whole.
Apprentices can demonstrate how they contribute to the wider business objectives and show an understanding of the wider business environments.	Understands the goals, vision and values of the organisation. Aware of the commercial objectives of the tasks/ projects they are working on. Understands the importance of meeting or exceeding customers' requirements and expectations. Is in tune with the organisation's culture.

Behaviour and relationship standard	Expected requirement
Apprentices can demonstrate the ability to use both logical and creative thinking skills when undertaking work tasks, recognising and applying techniques from both.	Logical thinking: • Recognises the conclusion to be reached; • Proceeds by rational steps; • Evaluates information, judging its relevance and value; • Supports conclusions, using reasoned arguments and evidence. Creative thinking: • Explores ideas and possibilities; • Makes connections between different aspects; • Embraces ideas and approaches as conditions or circumstances change.
Apprentices can show that they recognise problems inherent in, or emerging during, work tasks, and can tackle them effectively.	Problem-solving: • Analyses situations; • Defines goals; • Contributes to the development of solutions; • Prioritises actions; • Deals with unexpected occurrences.
Apprentices can manage relationships with work colleagues, including those in more senior roles, customers / clients and other stakeholders, internal or external, and as appropriate to their roles, so as to gain their confidence, keep them involved and maintain their support for the task / project in hand. Apprentices can establish and maintain productive working relationships, and can use a range of different techniques for doing so.	Managing relationships: • Understands the value and importance of good relationships • Acknowledges other people's accomplishments and strengths • Understands how to deal with conflict • Promotes teamwork by participating Customer/client relationships: • Understands their requirements, including constraints and limiting factors • Sets reasonable expectations • Understands how to communicate with them in decisions and actions • Interacts positively with them • Provides a complete answer in response to queries ('transparency', 'full disclosure') Stakeholders: • Understands who they are and what their 'stake' is

Behaviour and relationship standard	Expected requirement
	• Prioritises stakeholders in terms of their importance, power to affect the task and interest in it • Agrees objectives
Apprentices can communicate effectively with a range of people at work, one-to-one and in groups, in different situations and using a variety of methods. Apprentices can demonstrate various methods of communication, with an understanding of the strengths, weaknesses and limitations of these, the factors that may disrupt it, and the importance of checking other people's understanding.	Intention/purpose: • Understands the purpose of communicating in a particular situation or circumstance (e.g. inform, instruct, suggest, discuss, negotiate etc.) • Checks that the person/people with whom one is communicating also understand the purpose • Is sensitive to the dynamics of the situation • Is aware of anything that might disrupt the effectiveness of the communication (e.g. status, past history) Method: • Understands the most appropriate method for the situation • Aware of the limitations of the chosen method, and the possible risks of miscommunication (e.g. ambiguity) • Takes account of the affective dimensions of the method (e.g. body language, tone of voice, eye contact, facial expression etc.) Execution: • Expresses self clearly and succinctly, but not over-simplifying • Checks that the other person/people understand what is being expressed • Takes account of the potential barriers to understanding (e.g. filtering, selective perception, information overload) • Modifies the purpose and methods of communication during a situation in response to cues from the other person/people

These attributes are difficult to measure and are subjective in nature so cannot actually guarantee that any greater level of competence or proficiency is being demonstrated. The BCS Apprenticeship is mapped to the Skills Framework for the Information Age (SFIA), an internationally recognised skills framework and to observable activities that a cyber security technologist apprentice working to the level of responsibility appropriate for the role should demonstrate. Accordingly, the proficiencies that should be demonstrated by an apprentice in cyber security technologist are shown below.

Proficiency standard	Work activities demonstrating expected level of proficiency	Work activities demonstrating competence beyond the minimum expected
Business skills	Demonstrates an analytical and systematic approach to issue resolution. Takes the initiative in identifying and negotiating appropriate personal development opportunities. Demonstrates effective communication skills. Contributes fully to the work of teams. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures. Appreciates the wider business context, and how their role relates to other roles and to the business of the employer or client.	Selects appropriately from applicable standards, methods, tools and applications. Undertakes work that is more complex, more critical or more difficult. Demonstrates an ability to extend or enhance their approach to work and the quality of outcomes. Doesn't just solve the problem but explores all known options to do it better, more efficiently, more elegantly or better meet customer needs. Shows good project management skills, in defining problem, identifying solutions and making them happen.
Complexity	Performs a range of work, sometimes complex and non-routine, in a variety of environments. Applies a methodical approach to issue definition and resolution. Undertakes all work in accordance with agreed safety, technical and quality standards, using appropriate methods and tools.	Demonstrates a disciplined approach to execution, harnessing resources effectively. Drives solutions – with strong goal focused and appropriate level of urgency.
Influence	Interacts with and influences colleagues. Has working level contact with customers, suppliers and partners.	Externally – works with customers, suppliers, and partners in a variety of situations. Actively works with others and leads by example.

Proficiency standard	Work activities demonstrating expected level of proficiency	Work activities demonstrating competence beyond the minimum expected
	May supervise others or make decisions which impact the work assigned to individuals or phases of projects. Makes decisions which influence the success of projects and team objectives.	
Autonomy	Works under general direction. Uses discretion in identifying and responding to complex issues and assignments. Usually receives specific instructions and has work reviewed at frequent milestones. Determines when issues should be escalated to a higher level.	Internally – works alone, 1:1, in a team and with colleagues at all levels. Reads situation, adapts behaviours, and communicates appropriately for the situation and the audience. Can be trusted to deliver, perform and behave professionally, manages and delivers against expectations, proactively updates colleagues and behaves in line with the values and business ethics.

Cyber Security Technologist Apprentice Templates

The following templates are designed to support the training provider, and will take them from training and development planning, through to the end-point assessment readiness check. As with the tables above they can be used by the training provider to help them manage the process through to completion, although training providers may also substitute their own processes and documentation as they see fit in order to effectively manage their programme.

Cyber Security Technologist Template 1 – Training and Development Plan

Apprentice details

Name	
ULN number	

Employer details

Contact name	
Company name	
Company address	

Training provider details

Contact name	
Company name	
Company address	

Role mapping against the Cyber Security Technologist standard

For each area of technical and behavioural competence an overall evaluation should be provided on a three-point scale to show how often this competence is required during the normal work carried out by the employer:

- **critical** – this competence is applied most of the time;
- **desirable** – this competence is applied some of the time;
- **occasional** – this competence is rarely required.

This evaluation could form the basis of an ongoing review with the apprentice on a regular basis.

Workplace competence map

The template shows the type of activities that are identified in the apprenticeship standard for Cyber Security Technologist as demonstrating the required competencies being applied in the workplace.

It is recognised that there are differences between the types of work carried out by different employers, so this template provides the opportunity to include any other activity that demonstrates the apprentice's competence during their normal duties.

The tables below could be used to make an evaluation of the apprentice's work environment and detail the work activities that a competent apprentice should be able undertake. This activity should then lead to a discussion to identify any gaps with the employer and make a plan to redress the balance.

In the normal course of work, is the apprentice exposed/required to:	**Critical**	**Desirable**	**Occasional**
Threats, hazards, risks and intelligence	☐	☐	☐
Developing and using a security case	☐	☐	☐
Organisational context	☐	☐	☐
Future trends	☐	☐	☐
Design build and test a network	☐	☐	☐
Analysing a security case	☐	☐	☐
Structured and reasoned implementation of security in a network	☐	☐	☐

What is your overall evaluation of the apprentice's opportunity to demonstrate the technical competencies in the employer's normal workplace environment?

Please continue on a separate sheet if required.

Knowledge module training plan

The knowledge standards define learning that should take place during the apprenticeship, **both through the training provider activities and the apprentice's independent learning**. The training provider should work with the employer to identify appropriate training for the apprentice to meet the requirements of the standard and the employer should identify opportunities within the scope of their normal business activities for the apprentice to demonstrate what they have learnt.

Knowledge and understanding will be delivered through BCS qualifications and vendor certifications in accordance with the Cyber Security Technologist standard.

Training plan – knowledge

BCS qualification	**Completed Y/N**
BCS Level 4 Certificate in Cyber Security Introduction	
BCS Level 4 Certificate in Network and Digital Communications Theory	
BCS Level 4 Certificate in Security Case Development and Design Good Practice	
BCS Level 4 Certificate in Security Technology Building Blocks	
BCS Level 4 Certificate in Employment of Cryptography	

Technical competence development plan

The following template may be used to describe how to ensure that the apprentice will be given the opportunity to demonstrate each of the required technical competencies stated in the Cyber Security Technologist standard.

Competency requirement to meet the standard	**How will this be ensured?**	**Responsibility (employer or training provider)?**
Threats, hazards, risks and intelligence		
Developing and using a security case		
Organisational context		
Future trends		
Design build and test a network		
Analysing a security case		
Structured and reasoned implementation of security in a network		

Professional development activities plan

BCS has defined a number of professional development activities that support wider professional and career development. These activities have been associated with the various levels of responsibility, and the activities listed in the table below represent those that are appropriate for a cyber security technologist apprentice.

Training providers may wish to engage in assisting the apprentice in some of these activities as they can contribute towards the portfolio of evidence. The recommended activities include those shown below.

Professional development activities	**Appropriate to the role**	**Agreed with apprentice and employer**
Participating in group activities inside or outside the working environment that can assist with the development of interpersonal skills.	☐	☐
Undertaking unpaid activities that can help to develop professional skills or offer additional insight into, or understanding of, their working role.	☐	☐
Undertaking learning in subjects relevant to, but not directly related to, their role (e.g. mentoring skills, cultural awareness and diversity training), perhaps through self-study or evening classes.	☐	☐
Gaining basic knowledge of the employing organisation, its business, structure, culture, products/services, operations and terminology.	☐	☐
Gaining knowledge of IT activities in the employing organisation external to their function.	☐	☐
Exploring a topic that is not part of their normal responsibilities, and presenting findings to colleagues and/or management.	☐	☐
Attending meetings, seminars and workshops organised by a professional body, and reading published material such as journals and web content.	☐	☐
Undertaking learning and practice in the techniques of team and collaborative working. Gaining an understanding of the underlying concepts.	☐	☐
Undertaking learning and practice in oral and written communications, including report writing and presentations.	☐	☐

Cyber Security Technologist Template 2 – Weekly Diary

Week number	Activities completed	Competencies displayed	Supporting evidence

Cyber Security Technologist Template 3 – Periodic Workplace Competence Assessment and Remedial Action Plan

This template can be used to track the competencies being applied in the workplace on a continual / periodic basis. The training provider can then discuss any gaps with the employer and make a plan to redress the balance.

Competence assessment

In the normal course of work, is the apprentice demonstrating these competencies?	**Sufficiently applied to meet minimum competence standard**	**Start/stop/continue – what should the apprentice start, stop or continue doing in order to develop this competence?**
Threats, hazards, risks and intelligence	☐	
Developing and using a security case	☐	
Organisational context	☐	
Future trends	☐	
Design build and test a network	☐	
Analysing a security case	☐	
Structured and reasoned implementation of security in a network	☐	

Remedial action plan

An important function of the training provider is to act as an advisor to the apprentice and the employer to ensure that the programme remains on track and any concerns are addressed. The training provider should agree how best to provide ongoing assistance / advice throughout the apprenticeship, possibly as part of their contract / service agreement with the apprentice's employer.

If any remedial action is required, the table below could be used to record it.

Remedial action (if any) required to deliver the plan/SLA agreed with the employer and apprentice to demonstrate the technical competencies in the employer's normal workplace environment:
Please continue on a separate sheet as required.

Cyber Security Technologist – The Employer Reference Overview

This template and guidance will assist the training provider in supporting the employer when completing the employer reference, which forms a key part of the final end point assessment.

This employer reference template should be used to record the employer's comments against the grading minimum standards, criteria and dimensions, as set out in the Cyber Security Technologist standard.

For each area of technical competence and behavioural proficiency, the employer will be asked to provide an overall evaluation on a three-point scale:

- **Met** – they have observed this behaviour in the apprentice most of the time;
- **Exceeded** – they have observed this behaviour in the apprentice all of the time;
- **Not Met** – they have not observed this behaviour in the apprentice.

They should perform an evaluation using the checkboxes, and then provide an overall evaluation of the apprentice's competence or proficiency.

The template shows the type of activities that could demonstrate the required competencies and behaviours being applied in the workplace. There are always differences between individual employers and their requirements so there is the opportunity for the employer to include any other activity that they think demonstrates the apprentice's competence. It should be completed by a senior member of the team, who is able to comment directly on work activities.

Cyber Security Technologist Template 4 – The Employer Reference

Apprentice details

Name	
ULN number	

Training provider details

Contact name	
Company name	
Company address	

Employer details

Name	
Company address	
Signed by: Print name: Job title: Date:	

Section 1
Technical competence evaluation

Please provide your evaluation of the technical competence of the apprentice using the tables below. Under each heading is a list of activities that a competent apprentice should be able to demonstrate.

Please indicate your assessment of each competence using the checkboxes, and then provide an overall evaluation of the apprentice's technical competence:

Competence – Threats, Hazards, Risks and Intelligence

In your view, is the apprentice competent to:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
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 use of relevant external sources of threat intelligence or advice (e.g. CERT UK). 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?	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's competence in threats, hazards, risks and intelligence?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of competence in this area. Please continue on a separate sheet if required.

Competence – Developing and Using a Security Case

In your view, is the apprentice competent to:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
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)?	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's competence in recognises anomalies in observed network data structures?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of competence in this area. Please continue on a separate sheet if required.

Competence – Organisational context

In your view, is the apprentice competent to:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
Identify and follow organisational policies and standards for information and cyber security.	☐	☐	☐
Operate according to service level agreements or employer defined performance targets.	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's competence in accurately reports information?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of competence in this area.

Please continue on a separate sheet if required.

Competence – Future trends

In your view, is the apprentice competent to:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
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.	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's competence in recognises normal features of log files?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of competence in this area.

Please continue on a separate sheet if required.

Competence – Design Build and Test a Network

In your view, is the apprentice competent to:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
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.	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's competence in recognises main features of network layer?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of competence in this area.
Please continue on a separate sheet if required.

Competence – Analysing a Security Case

In your view, is the apprentice competent to:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
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.	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's competence in uses automated tools?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of competence in this area. Please continue on a separate sheet if required.

Competence – Structured and Reasoned Implementation of Security in a Network

In your view, is the apprentice competent to:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
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 relevant 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.	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's competence in undertakes root cause analysis?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of competence in this area.
Please continue on a separate sheet if required.

Section 2

Behaviours, business skills and level of responsibility evaluation

Please provide an evaluation as to the level of responsibility of the apprentice you are providing a reference for using the tables below. Under each heading is a list of proficiencies that a competent apprentice should display. Please indicate your assessment of the apprentice's proficiency using the checkboxes, and then provide an overall evaluation of the apprentice's proficiency.

Proficiency – Business Skills

In your view, is the apprentice proficient at:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
Demonstrating an analytical and systematic approach to issue resolution?	☐	☐	☐
Taking the initiative in identifying and negotiating appropriate personal development opportunities?	☐	☐	☐
Demonstrating effective communication skills?	☐	☐	☐
Contributing fully to the work of teams?	☐	☐	☐
Planning, scheduling and monitoring own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures?	☐	☐	☐
Appreciating the wider business context, and how own role relates to other roles and to the business of the employer or client.?	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's business skills?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of proficiency in this area. Please continue on a separate sheet if required.

Proficiency – Complexity

In your view, is the apprentice proficient at:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
Performing a range of work, sometimes complex and non-routine, in a variety of environments?	☐	☐	☐
Applying methodical approaches to issue definition and resolution?	☐	☐	☐
Undertaking all work in accordance with agreed safety, technical and quality standards, using appropriate methods and tools.	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's proficiency at handing complexity?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of proficiency in this area.
Please continue on a separate sheet if required.

Proficiency – Autonomy

In your view, is the apprentice proficient at:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
Working under general direction?	☐	☐	☐
Using discretion in identifying and responding to complex issues and assignments?	☐	☐	☐
Usually receiving specific instructions and has work reviewed at frequent milestones?	☐	☐	☐
Determining when issues should be escalated to a higher level?	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's proficiency to work autonomously?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of proficiency in this area.

Please continue on a separate sheet if required.

Proficiency – Influence

In your view, is the apprentice proficient at:	The apprentice has MET this requirement	The apprentice has EXCEEDED this requirement	The apprentice has NOT MET this requirement
Interacting with and influencing colleagues?	☐	☐	☐
Having working level contact with customers, suppliers and partners?	☐	☐	☐
Supervising others or make decisions which impact the work assigned to individuals or phases of projects?	☐	☐	☐
Making decisions which influence the success of projects and team objectives?	☐	☐	☐

- **Met** – you have observed this behaviour in the apprentice most of the time.
- **Exceeded** – you have observed this behaviour in the apprentice all of the time.
- **Not Met** – you have not observed this behaviour in the apprentice.

What is your overall evaluation of the apprentice's ability to influence?

Please give reasons, together with supporting examples, why you think the apprentice has demonstrated this level of proficiency in this area. Please continue on a separate sheet if required.

Section 3
Professional development

A number of professional development activities have been identified as part of the SFIA***plus*** framework to help career development. These activities have been associated with the various levels of responsibility, and the activities listed in the table below represent those that are appropriate for a cyber security technologist apprentice.

In your view, is the apprentice undertaking any of the following professional development activities:	**The apprentice is demonstrably undertaking this activity**	**The apprentice is NOT demonstrably undertaking this activity**
Participating in group activities inside or outside the working environment that can assist with the development of interpersonal skills?	☐	☐
Undertaking pro bono (unpaid) activities that can help to develop professional skills or offer additional insight into, or understanding of, their working role?	☐	☐
Undertaking learning in subjects relevant to, but not directly related to, their role (e.g. foreign language courses, mentoring skills, cultural awareness and diversity training), perhaps through self-study or evening classes?	☐	☐
Gaining basic knowledge of the employing organisation, its business, structure, culture, products/services, operations and terminology?	☐	☐
Gaining knowledge of IT activities in the employing organisation external to their function?	☐	☐
Exploring a topic that is not part of their normal responsibilities, and presenting findings to colleagues and/or management?	☐	☐
Attending meetings, seminars and workshops organised by a professional body and reading published material such as journals and web content?	☐	☐
Undertaking learning and practice in the techniques of team and collaborative working. Gaining an understanding of the underlying concepts?	☐	☐
Undertaking learning and practice in oral and written communications, including report writing and presentations?	☐	☐

What is your overall evaluation of the apprentice's ability to undertake wider professional development?

Please continue on a separate sheet if required.

Overall impressions and constructive feedback

This section is an opportunity for you to provide written feedback outside the rigid competency structure.

It is a free text field to allow you to share general thoughts on the apprentice's performance in case you were unable to say everything you wanted to say using the structured template. For example, you may want to highlight some of the areas where you have not been able to give the apprentice the exposure they would have liked.

We would welcome any general constructive development advice you may wish to give.

Please continue on a separate sheet if required.

Cyber Security Technologist Template 5 – Declaration and Evidence Checklists for the Completion of the Summative Portfolio

This template is to support the training provider in working with the apprentice and employer to ensure the successful completion of the summative portfolio

The checklists can be used by training providers to help them manage the process through to completion, although training providers may also substitute their own processes and documentation as they see fit.

The key responsibilities of the apprentice in producing their summative portfolio can be found in the General Guidance for Apprentices, Employers and Training Providers, as can generic guidance on how to select evidence to compile the summative portfolio.

The apprentice should gather artefacts and record information that can evidence their activities undertaken in the workplace. The portfolio of evidence should demonstrate the full range of competencies, as shown in this template, which are required by the standard to show that the apprentice can fulfil the role of a cyber security technologist.

Summative Portfolio Declaration

Apprentice declaration

Name	[first name] [surname]
ULN	[e.g.123456]
Declaration	[I confirm that all the evidence submitted is my own work and it has been completed as specified]
Signature	
Date	

Line manager declaration (employer)

Name	[line manager name]
Company	[employer name]
Declaration	I confirm that the work contained within this portfolio has, to the best of my knowledge, been completed solely by [apprentice's name]
Signature	
Date	

Training provider declaration (training provider)

Name	[observer name]
Company	[training provider name]
Declaration	I confirm that the work contained within this portfolio has, to the best of my knowledge, been completed solely by [apprentice's name]
Signature	
Date	

Cyber Security Technologist competencies evidence checklist

The defined competence areas and associated typical evidence are listed in this table. Not all employer businesses are identical so there will always be variation in the types of activity that will be carried out in the course of each apprentice's daily work; however, each cyber security technologist apprentice must be able to demonstrate evidence of every competence.

Competence		
Threats, hazards, risks and intelligence		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
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 the use of relevant external sources of threat intelligence or advice (e.g. CERT UK). 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.		

Competence		
Developing and using security case		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
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).		

Competence		
Organisational context		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
Identify and follow organisational policies and standards for information and cyber security.		
Operate according to service level agreements or employer defined performance targets.		

Competence		
Future trends		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
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 your business, with supporting reasoning.		

Competence		
Design, build and test a network		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
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.		
The apprentice should be able to provide evidence that the system meets the design requirement.		

Competence		
Analyse a security case		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
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.		
The apprentice should be able to identify conflicting requirements and propose, with reasoning, resolution through appropriate tradeoffs**.**		

Competence		
Implement security in a network (structured and reasoned)		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
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.		
The apprentice should be able to select and configure at least 2 types of common security hardware and software components to implement a given security policy.		
The apprentice should be able to design a system employing a crypto to meet defined security objectives. Develop and implement a key management plan for the given scenario/system.		

Generic levels of responsibility evidence checklist

Areas of responsibility and associated typical evidence are shown below.

Proficiency		
Business skills Demonstrates an analytical and systematic approach to issue resolution. Takes the initiative in identifying and negotiating appropriate personal development opportunities. Demonstrates effective communication skills. Contributes fully to the work of teams. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures. Appreciates the wider business context, and how their role relates to other roles and to the business of the employer or client.		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
Evidence that you can demonstrate an analytical and systematic approach to issue resolution.		
Evidence that you can take the initiative in identifying and negotiating appropriate personal development opportunities.		
Evidence that you can demonstrate effective communication skills.		
Evidence that you can contribute fully to the work of teams.		
Evidence that you can plan, schedule and monitor own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures.		
Evidence that you can appreciate the wider business context, and how your role relates to other roles and to the business of the employer or client.		

Proficiency		
Complexity Performs a range of work, sometimes complex and non-routine, in a variety of environments. Applies a methodical approach to issue definition and resolution. Undertakes all work in accordance with agreed safety, technical and quality standards, using appropriate methods and tools.		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
Evidence that you can perform a range of work, sometimes complex and non-routine, in a variety of environments.		
Evidence that you can apply a methodical approach to issue definition and resolution.		
Evidence that you undertake all work in accordance with agreed safety, technical and quality standards, using appropriate methods and tools.		

Proficiency		
Autonomy Works under general direction. Uses discretion in identifying and responding to complex issues and assignments. Usually receives specific instructions and has work reviewed at frequent milestones. Determines when issues should be escalated to a higher level.		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
Evidence that you can work under general direction.		
Evidence that you can use discretion in identifying and responding to complex issues and assignments.		
Evidence that you can usually receive specific instructions and have work reviewed at frequent milestones.		
Evidence that you can determine when issues should be escalated to a higher level.		

Proficiency		
Influence Interacts with and influences colleagues. Has working level contact with customers, suppliers and partners. May supervise others or make decisions which impact the work assigned to individuals or phases of projects. Makes decisions which influence the success of projects and team objectives.		
Minimum expected requirement	**List the evidence in the portfolio that fulfils this requirement**	**Reflections on applying knowledge learnt**
Evidence that you can interact with and influence colleagues.		
Evidence that you have working level contact with customers, suppliers and partners.		
Evidence that you may supervise others or make decisions which impact the work assigned to individuals or phases of projects.		
Evidence that you can make decisions which influence the success of projects and team objectives.		

Professional development activities evidence checklist

Areas of additional professional development activities that might be undertaken and associated typical evidence are shown below.

Professional development topic	Objectives	Typical evidence
Understanding organisation	Gaining basic knowledge of the employing organisation, its business, structure, culture, products/services, operations and terminology. Gaining knowledge of IT activities in the employing organisation external to their function.	• organisation charts; • company annual reports; • company website; • documents or reports from other areas of the business.
Additional business skills	Undertaking learning and practice in the techniques of team and collaborative working. Gaining an understanding of the underlying concepts. Undertaking learning and practice in oral and written communications, including report writing and presentations. Learning from experience and mistakes and applying the lessons as part of continuous improvement.	• presentations, reports or minutes of meetings that demonstrate communication skills, report writing abilities and collaborative activities; • evidence of reviewing their work and suggesting improvements or critically appraising what they did and what they learned from it.
External activities	Participating in group activities inside or outside the working environment that can assist with the development of interpersonal skills. Undertaking unpaid activities that can help to develop professional skills or offer additional insight into, or understanding of, their working role.	• evidence of meetings attended through continuous professional development records; • evidence of activities undertaken.

Additional learning	Undertaking learning in subjects relevant to, but not directly related to, their role (e.g. foreign language courses, mentoring skills, cultural awareness and diversity training), perhaps through self-study or evening classes. Exploring a topic that is not part of their normal responsibilities, and presenting findings to colleagues and/or management.	• evidence of learning undertaken from continuous professional development records; • evidence of presentations given to colleagues and/or management.
Professional networking	Attending meetings, seminars and workshops organised by a professional body and reading published material such as journals and web content.	• evidence of meetings attended through continuous professional development records; • written evidence summarising learning gained from reading.

Cyber Security Technologist Template 6 – End-Point Assessment Readiness Check

The training provider should assess whether the apprentice has met the criteria for the end-point assessment as defined in the standard.
The template below is a simple checklist that may be used.

Competence	Ready	Not ready	Comments
Threats, hazards, risks and intelligence	☐	☐	
Developing and using a security case	☐	☐	
Organisational context	☐	☐	
Future trends	☐	☐	
Design, build and test a network	☐	☐	
Analyse a security case	☐	☐	
Implement security in a network (structured and reasoned)	☐	☐	