BCS Digital Industries Apprenticeship

Standard Specific Guidance for Training Providers

Level 4 Cyber Security Technologist Apprenticeship – Technologist Specialism

Version 7.0
September 2020

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.
Version 6.0 August 2019	Complete document layout overhaul. Competencies and proficiencies unchanged.
Version 7.0 September 2020	Template 4&5 paragraph updated, learning outcomes updated in line with syllabus rework.

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 (Technologist specialism) apprenticeship. It should be read in conjunction with the Standard, Occupational Brief and Assessment Plan and is designed to give training providers some tools to help them build their own programme from training plan through to end point assessment (EPA).

This guide will provide supporting information around how to help the apprentice to meet and go beyond the standard and a number of useful documents to support the training provider in meeting their responsibilities in managing the apprenticeship from training plan through to the EPA.

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 BCS website provides the broad view on how to run an apprenticeship programme to the BCS Digital Industries Standard. 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 EPA.

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 EPA.

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 role of a Cyber Security Technologist is to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations systems and people.

Those focused on the technical side work on areas such as security design & architecture, security testing, investigations & response.

Those focussed on the risk analysis side focus on areas such as operations, risk, governance & compliance.

Whether focussed on the technical or risk analysis side, all people in this occupation work to achieve required security outcomes in a legal and regulatory context in all parts of the economy. They 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 & Compliance Analyst, Information Security Assurance & Threat Analyst, Forensics & Incident Response Analyst, Security Engineer, Information Security Auditor, Security Administrator, Information Security Officer.

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 (Technologist Specialism) – 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 assessment criteria 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 EPA. These knowledge standards, therefore, show the additional learning that may support the apprentice in improving their overall competence.
Technical knowledge and understanding are assessed throughout the apprenticeship through a combination of Ofqual regulated knowledge modules and/or specified vendor and professional qualifications which must be passed before the EPA can take place.

Qualification Name	IFA Knowledge Standard	Occupational Brief Expected Minimum Requirement	Assessment Criteria The Learner Can…
BCS Level 4 Certificate in Cyber Security Introduction	Why cyber security matters – the importance to business and society.	• Explain why information and cyber security is important to business and society.	Describe what information assets and information processing systems are.
			Explain why information assets and related systems need to be protected.
			Describe the impact, negative or positive, a security incident could have on an organisation. • Financial; • Operational; • Reputational; • Legal; • Regulatory.
			Discuss how information and cyber security impacts different types of organisations. • Public; • Private; • CNI; • Different industries; • Different geographical locations; • Large enterprise; • Small business; • Charity/non-profit.
			Describe how information and cyber security can affect society: • Citizens;

			• Not for profit groups; • Public services.
	Basic theory – concepts such as security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard. Also how these relate to each other and lead to risk and harm.	• Explain basic concepts: security, identity, confidentiality, integrity, availability, threat, vulnerability, risk & 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 & motive) examples of threats and also describe some typical hazards that may concern an organisation. Recognise that	Describe confidentiality, integrity, availability, identity, authentication and nonrepudiation.
			Explain how threats and vulnerabilities create risk.
			Explain how likelihood and impact are used to determine risk and how this is recorded. • Risk register.
			Describe how defending information assets and related systems is asymmetric because every risk needs to be treated whilst attackers only need to exploit one.
			Describe sources of threats and their capability, motivations and opportunity. • Individuals; • Groups (criminal and political); • Nation states; • Insiders (deliberate or accidental).
			Describe how environmental hazards and inadequate system design and maintenance create risks.
			Explain how the organisation's culture and security objectives govern the types of controls selected.

		there are different types or classes of threat 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 cybersecurity risk assessment, taking account the wider business risk context.	Explain how risk appetite is determined and what risk treatment options are available. • Accept; • Reduce; • Avoid; • Transfer or share.
	Security assurance – concepts (can explain what assurance is for in security, and 'trustworthy' versus 'trusted') and how assurance may be achieved in practice (can explain what penetration testing is and how it contributes to assurance; and extrinsic assurance methods).	• 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 & implementation, operational policy & 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	Explain what 'trusted' (e.g. proven through the use of PKI certificates) and 'trustworthy' (e.g. implied by the use of secure development methodologies) mean when applied to information security assurance. Explain what is meant by the following approaches to assurance and describe when they can be used: • Intrinsic assurance (confidence in the process used by the supplier during development by following a recognised standard); • Extrinsic assurance (independent of the development environment using external evaluation); • Design & implementation (designed and implemented to a recognised standard);

		system of extrinsic assurance (e.g. security testing, supply chain assurance, Common Criteria) explaining the benefits and limitations. Describe at least 2 ways an organisation can provide intrinsic assurance.	• Operational policy & process (operated and maintained to a recognised standard).
			Explain that penetration testing is a form of assurance ideally carried out by professionals using industry recognised ethical methods to test the technical and organisational controls in place. • Pen test; • Red team exercise; • Bug/bounty hunter.
			Describe the benefits and limitations of extrinsic assurance methods. • Security testing (an automated review against known vulnerabilities only); • Supply chain testing (point in time audit of suppliers' technical and organisational controls against a recognised standard of their compliance with legal and regulatory requirements); • Common criteria (a review of the organisations requirements against a standard specific to the technology).
			Describe ways an organisation can use intrinsic assurance. • What certificates does the supplier hold e.g. ISO27001. ISO9001;

			• What standards have a supplier's products been certified against e.g. FIPS.
	How to build a security case – deriving security objectives with reasoned justification in a representative business scenario	• Derive and justify security objectives. Describe how these might apply to information and infrastructure assets in at least 2 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.	Describe what security objectives and security requirements are and what they should include: • Functional requirements; • Non-functional requirements; • Relative priority (MoSCoW); • KPI's; • Responsibility.

			Justify how security objectives are applied to information assets and infrastructure assets in different business scenarios depending on the value of the asset and the part the asset plays in the scenario. • Migrating from an on-premise solution to a cloud service; • Developing a new product that uses customer data; • Outsourcing key business process.
	Cyber security concepts applied to ICT infrastructure – can describe the fundamental building blocks and typical architectures and identify some common vulnerabilities in networks and systems.	• 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.	Describe common vulnerabilities in computer network and systems: • Non-secure coding; • Inadequate traffic filtering; • Missing patches and updates; • Inappropriate configuration; • Insecure protocols; • Lack of malware protection; • Inadequate access controls (identification, authentication, authorisation, ACLs); • Inappropriate design and architecture; • Lack of consideration of environmental factors; • Inadequate physical security controls; • Interoperability.

			Describe the building blocks of computers, networks and the internet: • Input devices; • Output devices; • Routers; • Switches; • Hubs; • Wireless access points and controllers; • Clients and servers; • Local and networked storage; • Network transmission media; • Industrial control systems; • Data centres.
			Describe typical architectures of computers, networks and the internet. • Wireless and wired; • Operating systems; • Fat and thin clients; • Physical and virtual; • Hub and spoke; • Mesh network; • Redundant hardware and transmission paths.
	Attack techniques and sources of threat – can describe the main	• Describe the main different types of common attack techniques (for example: phishing, social	Describe the main attack techniques and explain how they work and where are successful: • phishing and its variations;

	types of common attack techniques; also the role of human behaviour. Explain how attack techniques combine with motive and opportunity to become a threat.	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)	• social engineering; • malware; • network interception; • advanced persistent threats; • DOS and DDOS; • Physical theft; • Business email compromise.
			List insider threats • Malicious employee; • Negligent employee; • Inadequately trained employee; • Unmanaged 3rd party staff.
			Describe the factors that contribute to a negative or positive cyber security environment. • Management direction through policy; • Communication; • Training and awareness; • Incident reporting; • Roles and responsibilities; • Whistleblowing.
			Explain how a threat is the results of an attack technique combined with the motive and opportunity. • Motive; ○ Criminal;

			○ Political; ○ Reputational. • Opportunity; ○ M&A; ○ Fluctuations in currency or asset value; ○ Changes to technology; ○ Change in personnel; ○ Changes in political landscape; ○ New vulnerabilities in products disclosed.
			Describe how environmental hazards such as fire and flood can results in the same impact as an attack.
	Cyber defence – describe ways to defend against attack techniques.	• Describe ways to defend against the main attack techniques, including consideration of 'deter', 'protect', 'detect' & 'react' and an 'attack chain'.	List the main defensive techniques, classify them as deter protect, detect or react and describe how they can be used together to create defence in depth. • Perimeter controls; • Traffic filtering; • Least privilege; • Authentication and authorisation; • Anti- malware; • Application whitelisting; • Proactive monitoring; • Secure configuration; • Intrusion detection and prevention;

			• File integrity monitoring; • Data loss prevention; • Patching and updating; • Change control; • Encrypted connections.
			Describe the benefits of using the MITRE ATT&CK model. • Initial access; • Execution; • Persistence; • Privileged escalation; • Defence evasion; • Credential access; • Discovery; • Lateral movement; • Collection; • Exfiltration; • Command and control.
	Relevant laws and ethics – describe security standards, regulations and their consequences across at least two sectors; the role of criminal and other law; key	• Describe the cyber security standards and regulations and their consequences for at least 2 sectors (e.g. Government, finance, petrochemical/process control), comparing and contrasting the differences.	Describe the cyber security standards and regulations and their consequences for the following sectors: • Government (HMG Security Policy Framework, Cyber Essentials); • Finance (PCI-DSS, NIST, ISO27001, FCA, PRA, CBEST);

	relevant features of UK and international law.	• Appreciate the role of criminal law, contract law and other sources of regulation. • Explain the benefits & 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), e.g.: Computer Misuse Act, Data Protection Act, Human Rights Act. • Describe the implications of international laws and regulations that affect organisations, systems and users in the UK, movement of data and equipment	• Defence (Def Stan 05-138, JSP440, JSP604, NIST) • CNI (NISD, Operational Guidelines for Industrial Automated Control Systems (ICAS). Explain the role of laws and regulations on cyber security with reference to: • Criminal law (e.g. Computer Misuse Act, Data Protection Act): • Contract law (service delivery management and meeting SLAs); • Industry specific regulations (e.g. finance, health). Explain the benefits, costs and motives for uptake of security standards by organisations including: • PCI-DSS; • ISO27001; • Cyber Essentials.

		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 1 generally recognised and relevant professional body the ethical responsibilities of a cyber-security professional.	Describe the key features of relevant UK law that affect cyber security for individuals and organisations including; • Computer Misuse Act; • Data Protection Act; • Human Rights Act; • Copywrite, Designs and Patents Act.
			Describe the key features of relevant international laws and regulations and their implications for cross border movement of data and products including: • Digital Millennium Act; • ITAR; • EU-US Privacy Shield (replaced Safe Harbour); • General Data Protection Regulation; • Patriot Act.
			Describe the legal responsibilities of systems users and how the following are used to communicate them: • Acceptable use policies; • Logon banners; • Training and awareness programmes.
			Describe the ethics and codes of conduct for cyber security professionals with reference to following professional bodies:

			• BCS; • CIISec (formally IISP); • ISACA; • (ISC).
	The existing threat landscape – can describe and know how to apply relevant techniques for horizon scanning including use of recognised sources of threat intelligence.	• 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, online for a, 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 1 technique to identify trends in research. Illustrate with an example.	Describe horizon scanning with reference to the following source types: • Market trend reports (vendor reports, Gartner, ISF); • Academic research papers; • Professional journals (e.g. IEEE, IET, Oxford Academic, BCS); • Hacker conferences (e.g BlackHat, Bsides); • Government sponsored, online sources (e.g. CiSP, ENISA).
			Describe diversity when using horizon scanning with reference to: • Delphi method; • Trend impact analysis.
	Threat trends – can describe the significance of identified trends in	• Describe the significance of some identified trends in cyber security and	Describe trends in cyber security and their significance. • IoT security; • AI;

	cyber security and understand the value and risk of this analysis	understand the value and risk of this analysis.	• Quantum computing. Explain the value and risk of analysing future trends. • Future proofing investment in technology; • Including future security requirements when planning changes and upgrades; • Under investing in categories of controls; • Training cyber security professionals in the right skills.

BCS Level 4 Certificate in Network and Digital Communications Theory	Understands the basics of networks: data, protocols and how they relate to each other; the main routing protocols; the main factors affecting network performance including typical failure modes in protocols and approaches to error control.	• 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	Describe the OSI and TCP/IP models and example protocols.
			• Application:
			  ○ HTTP/S;
			  ○ SNMP;
			  ○ SMTP.
			• Transport;
			  ○ TCP;
			  ○ UDP.
			• Internet:
			  ○ IPv4 and IPv6;
			  ○ ICMP.
			• Link:
			  ○ Ethernet.
			
			Explain what a network protocol is and how it transmits data with reference to:

		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.	• Host addressing; • Frames; • Packets; • Datagrams; • Data.
			Describe how protocols can fail and give examples of communication errors at different OSI layers. • Failure to find a route to a host; • Failure to negotiate an encryption method; • Failure to receive or acknowledge packets; • Failure to agree packet formats; • Failure to agree transmission speed or duplex models.
			Describe how error controls is applied to protocols.
			Explain what a routing protocol does and the difference between static and dynamic routing.

			Describe the main routing protocols in current use, describing the pros and cons of each and when they are used: • RIPv2 and RIPng; • OSPF; • BGP; • EIGRP; • IS-IS.
		• Explain some of main factors that affect network performance (e.g. the 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 prohibit streaming protocols).	Explain how network performance can be affected by various factors including: • Available bandwidth; • Number of users; • Applications in use; • WAN connection.
			Describe ways to improve network performance including: • Using QOS; • Traffic shaping and throttling; • Increasing local capacity; • Reducing WAN contention; • Increasing network bandwidth; • Using VLANs; • Restricting application use;

			• Restricting traffic at the border.
BCS Level 4 Certificate in Security Case Development and Design Good Practice	Understands, at a deeper level than from Knowledge Module 1, how to build a security case: describe what good practice in design is; describe common security architectures; be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance. Understand how to build a security case including context, threats, justifying the selected mitigations and security controls with reasoning and recognising the dynamic and	• Describe what good practice in design is and how this may contribute to security. [Use/refer to: Trustworthy Software Initiative (TSI) training material].	Describe the features of good systems design and explain how these contribute to security: • OWASP Security by Design Principles: ○ Minimize attack surface area; ○ Establish secure defaults; ○ Principle of least privilege; ○ Principle of defence in depth; ○ Fail securely; ○ Don't trust services; ○ Separation of duties; ○ Avoid security by obscurity; ○ Keep security simple; ○ Fix security issues correctly.
			Describe the facets of software trustworthiness as defined by The Trustworthy Software Framework and explain how each can be explicitly and implicitly assessed against an organisation's security requirements: • Safety; • Reliability; • Availability; • Resilience;

	adaptable nature of threats.		• Security.
			Explain the four levels of trustworthiness, how the control sets apply and explain under what circumstances each might be appropriate. • TL1 Essential Practices; • TL2 Assessed Practices; • TL3 Enhanced Practices; • TL4 Specialist Practices.

		• 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).	Explain the purpose and nature of security architecture and how it differs from enterprise architecture considering all the technology, people and processes relating to a computer system.
			• NCSC secure design principles:
			  ○ Establish the context;
			  ○ Making compromise difficult;
			  ○ Making disruption difficult;
			  ○ Making compromise detection easier;
			  ○ Reducing the impact of compromise.

			Explain the common security architecture frameworks in use. • TOGAF; • MODAF; • Zachman; • SABSA; • NIST;

			• COBIT.
			List reputable sources of architectural patterns and guidance. • NCSC; • NIST; • Vendors.
		• 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.	Describe the purpose of a security case.
			List the key characteristics of a security case. • Business contexts; • Security objectives; • Threats and vulnerabilities; • Mitigation options; • Technical controls; • Organisational controls; • Cost benefit considerations; • Legal and regulatory environment; • Implantation activities.
			Describe the resources available to aid with development of a security case and how they can be used. • Common Criteria; • FIPS 140; • NCSC CAPS.

			Describe how threats can be modelled using the STRIDE example. • Spoofing; • Tampering; • Repudiation; • Information disclosure; • Denial of service; • Elevation of privilege.
			Describe how threats change in response to security architecture and how threat modelling may need to change as a result of the outcome.
BCS Level 4 Certificate in Security Technology Building Blocks	Understands how cyber security technology components are typically deployed in networks and systems to provide security functionality including: hardware and software.	• 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 account the implicit assurance (including supplier assurance and considering the benefits and risks of open source	Describe the main categories of security hardware and software that are available to assist with risk mitigation. • Network protection; ○ Network firewalls (perimeter, internal, DMZ); ○ IDS / IPS; ○ Web security / proxy; ○ Email security / MTA; ○ DNS filtering; ○ UTM; ○ Web application firewalls; ○ DLP; • Host protection; ○ Antivirus / anti-malware / EDR; ○ HIDS;

		options) of the component, describing any residual risks.	○ Software policies and permissions; • Proactive monitoring; ○ SIEM; ○ FIM; ○ Network traffic monitoring; ○ Honeypots; • Encryption technology; ○ WDE; ○ File encryption; ○ Message / traffic encryption; ○ Database encryption; ○ Removable media encryption; ○ HSM; ○ TPM; • Identify and access management; ○ Authentication technologies; ○ Authorisation; ○ Access controls (physical, NAC, ACLs); ○ Enterprise IDM solutions.
		• 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	Explain how each security hardware and software category listed helps to protect data and systems explaining what threat or vulnerability they are designed to address. Explain how the security hardware and software category listed is employed as part of a defence in depth approach with reference to the stages of the

		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 account the implicit assurance (including supplier assurance and considering the benefits and risks of open source options) of the component, describing any residual risks. • 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	attack chain they are designed to address using the MITRE ATT&CK model. • Initial access; • Execution; • Persistence; • Privileged escalation; • Defence evasion; • Credential access; • Discovery; • Lateral movement; • Collection; • Exfiltration; • Command and control. Describe how implicit assurance can be used to help select security hardware and software in different situations. • What security certifications does the supplier hold; • What frameworks or standards do they claim to follow; • What industry specific standards or codes of practice do they adhere to; • What do industry analysts and other customers say about the organisation or products; • What standards have a supplier's products been certified against.

		disk encryption, TLS, SSL, privacy enforcing technology) and the practical issues	Describe the limitations of the various security hardware and software categories listed and the common ways in which they can be defeated by skilled and determined adversaries.

		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.	Explain the benefits and risks of selecting open source solutions as part of a security strategy. • Free licence; • Auditable; • Editable / configurable; • Community support; • Lack of SLA for support and maintenance; • May include untrustworthy code.
BCS Level 4 Certificate in	Understands the basics of	• Describe the main cryptographic techniques (e.g. symmetric,	Describe the main cryptographic techniques in use. • Symmetric;

Employment of Cryptography	cryptography – can describe the main techniques, the significance of key management, appreciate the legal issues.	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.	○ Stream ciphers (e.g. RC4, ChaCha); ○ Block ciphers (e.g. RC5, AES, 3DES, Blowfish); • Asymmetric or public key; ○ RSA; ○ Diffle-Hellman; ○ PGP; ○ Elliptic curve ciphers; • Hashing; ○ MD5; ○ SHA.
			Describe how the main cryptographic techniques are used and the limitations of each in those situations. • File and disk encryption; ○ Removable media; ○ WDE for storage in desktops and servers; ○ Mobile phones; ○ Individual document encryption; • Database encryption; ○ Individual fields or records; ○ Transparent whole database encryption; • Digital rights management; ○ Product keys; ○ Copy protection for electronic media;

			○ DVD encryption; ○ Online authentication or activation; • Ransomware; ○ Removing access to files; ○ Key recovery; • Ecommerce; ○ TLS/SSL protected transactions; ○ Cryptocurrency; • Wireless communications; ○ WLANs; ○ Wireless WAN backhaul; • Email; ○ Message encryption; ○ Message signing; • Data destruction; ○ Destroying keys to remove access to data; ○ Blockchain. • Protecting passwords and other authentication mechanisms; ○ Hashing passwords; ○ Password managers; ○ Protecting biometrics; ○ Smart cards; • VPNs; ○ User authentication; ○ Network to network authentication;

			○ Traffic encryption.
			Explain how crypto systems are attacked. • Replay attacks; • Side channel; • Traffic analysis; • Brute force; • MTM; • Key theft.
			Explain how crypto systems and algorithms become obsolete and can be poorly implemented. • DES; • WEP; • MD5; • SHA1.
			Describe the features of key management including the key lifecycle and the challenges associated with each stage. • Generate; • Distribute; • Deploy; • Archive; • Revoke; • Destroy.

			Explain how key management works in symmetric and asymmetric cryptosystems describing the benefits and limitations of each. • Open and closed source key management systems; • Cloud based key management services; • PKI and digital certificates.
			Explain the significance of entropy in cryptography.
		• Describe the role of cryptographic techniques in a range of different systems (e.g. GSM, Chip&PIN, common hard disk encryption, TLS, 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.	Describe how cryptographic techniques are used in different systems and the practical difficulties of each in those situations including how to introduce and maintain them in an existing ecosystem. • Cellular radio e.g. GSM and professional radio e.g. TETRA; • Chip and PIN enabled payment cards; • Authentication tokens; • File and desk encryption in desktop operating systems; • Online transactions using TLS/SSL; • 'chat' communications e.g. Whatsapp, iMessage; • Password managers.
			Recognise that there are legal issues surrounding cryptography when crossing national borders or exporting / importing cryptographic technology.

			Describe the purpose of the Wassenaar Arrangement and how it impacts on cryptography.

Table 2 – Cyber Security Technologist (Technologist Specialism) – 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 all the competencies below.

The BCS apprenticeship is mapped to an internationally recognised skills framework and to work activities in which the apprentice would be involved. The following tables set out these competencies and the expected requirements against the work activities that might be demonstrated at and beyond the minimum expectation:

Competency Standard (IfATE Standard)	Expected Requirement (Occupational Brief)	Work Activities Demonstrating Expected Level of Competence
React to threats, hazards, risks and intelligence.	The apprentice should be able to: • Discover (through a mix of research and practical exploration) vulnerabilities in a system. • Analyse and evaluate security threats and hazards to a system or service or processes. Be aware of and demonstrate relevant external sources of threat intelligence or advice (e.g. CERT UK) and combine different sources to create an enriched view. • Research and investigate some common attack techniques and recommend how to defend against them. Be aware of and demonstrate use of relevant external sources of vulnerabilities (e.g. OWASP). • Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.	Reviews network usage. Assesses the implications of any unacceptable usage and breaches of privileges or corporate policy. Recommends appropriate action.

Competency Standard (IfATE Standard)	Expected Requirement (Occupational Brief)	Work Activities Demonstrating Expected Level of Competence
Develop and use a security case.	The apprentice should be able to: • Source and analyse a security case (e.g. a Common Criteria Protection Profile for a security component) and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern. • Develop a simple security case without supervision. (A security case should describe the security objectives, threats, and for every identified attack technique identify mitigation or security controls that could include technical, implementation, policy or process).	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.
Support the organisation.	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.
Identify future trends.	The apprentice should be able to investigate different views of the future (using more than one external source) and trends in a relevant technology area and describe what this might mean for a business, with supporting reasoning.	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.

Competency Standard (IfATE Standard)	Expected Requirement (Occupational Brief)	Work Activities Demonstrating Expected Level of Competence
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.
Analyse a security case.	The apprentice should be able to: • Analyse security requirements (functional and non-functional security requirements that may be presented in a security case) against other design requirements (e.g. usability, cost, size, weight, power, heat, supportability etc.), given for a given system or product. • Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.	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 (IfATE Standard)	Expected Requirement (Occupational Brief)	Work Activities Demonstrating Expected Level of Competence
Implement security in a network (structured and reasoned).	The apprentice should be able to: • Design and build a simple system in accordance with a simple security case. Provide evidence that the system has properly implemented the security controls required by the security case. The system could be either at the enterprise, network or application layer. • Select and configure at least 2 types of common security hardware and software components to implement a given security policy. • Design a system employing a crypto to meet defined security objectives. Develop and implement a key management plan for the given scenario/system.	Contributes to the development of solution architectures in specific business, infrastructure or functional areas, using appropriate tools and methods.

Below are the criteria for demonstrating if the apprentice is working at a significantly higher level than the expected level of competence:

Criteria for Demonstrating Significantly Higher Competencies.	Key Indicators
Understands and applies a wide range of tools and methods.	This must be in addition to the range of tools required for a pass and demonstrate solid breadth and depth of knowledge, application and purpose of the tools used.
Accurately and appropriately applies and effectively implements the right tools and methods in a variety of different situations.	These situations / tasks must show a wide range and breadth of situations and be in addition to normal day to day work
A capable user - exploits the functionality/capability of the tools and methods.	This must demonstrate solid breadth and depth of functionality, application and purpose of the tools selected. That they have researched and understood the rational for use and not just taken directions from others in the selection.
Broad understanding of different tools and methods and how and why they can be applied in different contexts.	This must demonstrate breadth and depth of the tools selected, why they have been selected and their appropriateness for the different tasks and uses.
Deals confidently and capably with interrelated and interdependent factors in their work.	This must demonstrate a confident and consistent approach to all areas of their work (both mundane and interesting work). They should have a thorough understanding and appreciation of their reliance and actions on others 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. 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 their role in 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.

Behaviour and Relationship Standard	Expected Requirement
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; • Prioritises stakeholders in terms of their importance, power to affect the task and interest in it; • Agrees objectives.

Behaviour and Relationship Standard	Expected Requirement
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 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 an apprentice working to the level of responsibility appropriate for the role should demonstrate. Accordingly, the proficiencies that should be demonstrated by the apprentice are shown below.

Proficiency Standard	**Work Activities Demonstrating Expected Level of Competence**
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.
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.
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.

Proficiency Standard	Work Activities Demonstrating Expected Level of Competence
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.

Below are the criteria for demonstrating if the apprentice is working at a significantly higher level than the expected level of proficiency:

Proficiency Standard	Work Activities Demonstrating Competence Beyond the Minimum Expected
Business skills	Works independently and takes responsibility. 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	Demonstrates a disciplined approach to execution, harnessing resources effectively. Drives solutions – with strong goal focused and appropriate level of urgency.
Influence	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 Competence Beyond the Minimum Expected
Autonomy	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 (Technologist Specialism) Apprentice Templates

The following templates are designed to support the training provider, and will take them from training and development planning, through to the EPA 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.

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 (Technologist Specialism) 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:

- competence is applied most of the time;
- competence is applied some of the time;
- competence is rarely required.

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

Workplace Competence Map

This template shows the type of activities that are identified in the apprenticeship standard.

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 to undertake. This activity should then lead to a discussion to identify any gaps with the employer and make a plan to redress the balance.

	Is the apprentice required to demonstrate the competency in the normal course of work?		
Competency Standard	**Most of the Time**	**Some of the Time**	**Rarely**
React to threats, hazards, risks and intelligence.	☐	☐	☐
Develop and use a security case.	☐	☐	☐
Support the organisation.	☐	☐	☐
Identify future trends.	☐	☐	☐
Design, build and test a network.	☐	☐	☐
Analyse a security case.	☐	☐	☐
Implement security in a network (structured and reasoned).	☐	☐	☐

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 in accordance with the standard.

Training Plan – Knowledge

BCS Qualification	Completed
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 ensure that the apprentice will be given the opportunity to demonstrate each of the required technical competencies stated in the standard.

	Responsibility	Employer ☐	Training Provider ☐
React to threats, hazards, risks and intelligence.			
How will this be ensured?			

	Responsibility	Employer ☐	Training Provider ☐
Develop and use a security case.			
How will this be ensured?			

	Responsibility	Employer ☐	Training Provider ☐
Support the organisation.			
How will this be ensured?			

	Responsibility	Employer ☐	Training Provider ☐
Identify future trends.			
How will this be ensured?			

	Responsibility	Employer ☐	Training Provider ☐
Design, build and test a network.			
How will this be ensured?			

	Responsibility	Employer ☐	Training Provider ☐
Analyse a security case.			
How will this be ensured?			

	Responsibility	Employer ☐	Training Provider ☐
Implement security in a network (structured and reasoned).			
How will this be ensured?			

Template 2 – Weekly Diary

Week number	Activities completed	Competencies displayed	Supporting evidence

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

	Is the apprentice meeting the minimum competence standard? ☐
React to threats, hazards, risks and intelligence.	
What should the apprentice start, stop or continue doing in order to develop this competence?	

	Is the apprentice meeting the minimum competence standard? ☐
Develop and use a security case.	
What should the apprentice start, stop or continue doing in order to develop this competence?	

	Is the apprentice meeting the minimum competence standard? ☐
Support the organisation.	
What should the apprentice start, stop or continue doing in order to develop this competence?	

Is the apprentice meeting the minimum competence standard?	☐

Identify future trends.
What should the apprentice start, stop or continue doing in order to develop this competence?

Is the apprentice meeting the minimum competence standard?	☐

Design, build and test a network.
What should the apprentice start, stop or continue doing in order to develop this competence?

Is the apprentice meeting the minimum competence standard?	☐

Analyse a security case.
What should the apprentice start, stop or continue doing in order to develop this competence?

	Is the apprentice meeting the minimum competence standard?	☐
Implement security in a network (structured and reasoned).		
What should the apprentice start, stop or continue doing in order to develop this competence?		

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.

Please continue on a separate sheet as required.

Template 4 – 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 EPA. The intent of the employer reference is for the employer to support the apprentice by validating the evidence that they have submitted for EPA.

The employer will be asked to provide an overall evaluation of the apprentice for each area of technical competence and behavioural proficiency, giving detail of how the apprentice meets each requirement.

This guidance 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.

The apprenticeship standards are designed to cover a wide range of different job roles. If the evidence in the portfolio is weak due to limited exposure within the day to day activities of the workplace, the synoptic project should be considered and selected to allow the apprentice to demonstrate that they are competent in those criteria and to provide the breadth and depth to meet the specified minimum requirements of the Occupational Brief.

The template is provided as a standalone editable document and can be found on the BCS Accredited Provider area. This should be completed by the employer and submitted for review as part of the EPA.

Template 5 – Summative Portfolio Checklist

This template will 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 apprentice should gather artefacts and record information that can evidence their activities undertaken in the workplace. The portfolio of evidence should demonstrate that the apprentice can fulfil the full range of competencies which are required by the standard, as shown in this template.

The apprenticeship standards are designed to cover a wide range of different job roles. If the evidence in the portfolio is weak due to limited exposure within the day to day activities of the workplace, the synoptic project should be considered and selected to allow the

apprentice to demonstrate that they are competent in those criteria and to provide the breadth and depth to meet the specified minimum requirements of the Occupational Brief.

The template is provided as a standalone editable document and can be found on the BCS Accredited Provider area.

Template 6 – EPA Readiness Check

This template is to support the training provider in assessing whether the apprentice has met the criteria for the EPA, as defined in the standard.

	Is the apprentice ready? ☐
React to threats, hazards, risks and intelligence.	
Comments	

	Is the apprentice ready? ☐
Develop and use a security case.	
Comments	

	Is the apprentice ready? ☐
Support the organisation.	
Comments	

	Is the apprentice ready? ☐
Identify future trends.	
Comments	

	Is the apprentice ready? ☐
Design, build and test a network.	
Comments	

	Is the apprentice ready? ☐
Analyse a security case.	
Comments	

	Is the apprentice ready?	☐
Implement security in a network (structured and reasoned).		
Comments		

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 an 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.	☐	☐

Activities Typical Evidence

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 pro bono (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.

Professional Development Topic	Objectives	Typical Evidence
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.