# BCS Digital Industries Apprenticeship

# Standard Specific Guidance for Training Providers

# Level 4 Cyber Security Technologist Apprenticeship – Technologist Specialism

# Version 6.0
# August 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. |
| Version 6.0 August 2019 | Complete document layout overhaul. Competencies and proficiencies unchanged. |

# 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 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. |
| | 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.<br>• 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 | Recall and explain key terminology. This could include:<br>• Security<br>• Identity<br>• Confidentiality<br>• Integrity<br>• Availability<br>• Threat<br>• Vulnerability<br>• Risk and hazard |
| | | | Describe what security is, fundamentally, by explaining:<br>• How the concepts of threat, hazard and vulnerability relate to each other and lead to risk<br>• The inherent asymmetric nature of cyber security threats |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | tool (e.g. a risk register).<br>• Understand the inherent asymmetric nature of cyber security threats.<br>• 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 there are different types or classes of threat and threat actor and that these may be profiled. Relate these descriptions to example security objectives.<br>• Understand how an organisation balances business drivers with the outcome and recommendations of a cybersecurity risk assessment, taking account the wider business risk context. | Describe and explain:<br>• What risk is<br>• How risks are usually quantified (by likelihood and relative impact)<br>• The use of at least one commonly used tool for risk management; such as a risk register |
| | | | Describe typical threats, threat actors and hazards in terms of capability, opportunity and motive using examples that may concern an organisation. These may include:<br>• Profiling techniques<br>• 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. |
| | Security assurance – concepts (can explain what assurance is for in security, and 'trustworthy' versus 'trusted') and how | • Assurance concepts: Explain the difference between 'trusted' and 'trustworthy' and explain what assurance is for in security. Describe the main approaches to | Recall, describe and explain security assurance concepts and how these might be applied at different stages in the lifecycle of a system; including:<br>• The difference between 'trusted' and 'trustworthy'<br>• The purpose of security assurance |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | assurance may be achieved in practice (can explain what penetration testing is and how it contributes to assurance; and extrinsic assurance methods). | 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.<br>• 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 2 ways an organisation can provide intrinsic assurance. | • The main approaches to:<br>o Assurance<br>o Intrinsic and extrinsic<br>o Design and implementation<br>o 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'. |
| | | | Describe at least one current system of extrinsic assurance, explaining the benefits and limitations. For example:<br>• Security testing<br>• Supply chain assurance<br>• Common criteria |
| | | | Describe at least two ways an organisation can provide intrinsic assurance. |
| | How to build a security case – deriving security objectives with reasoned justification | • Derive and justify security objectives. Describe how these might apply to information and infrastructure assets in at least 2 different and representative | 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. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | in a representative business scenario | 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. | 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.<br><br>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. |
| | 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).<br>• 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. | Show an understanding of common vulnerabilities in computer networks and systems. This may include, non-secure coding and unprotected networks.<br><br>Describe the fundamental building blocks of:<br>• Infrastructure elements; including:<br>o Firewalls<br>o Routers<br>o Switches<br>o Hubs<br>o Storage<br>o Transmission<br>• Typical architectures of computers, networks and the Internet, including:<br>o Server / client<br>o Hub / spoke<br>o Non-virtual/ virtual |
| | Attack techniques and sources of threat – | • Describe the main different types | Describe and explain the main types of attack techniques. For each type of attack, apprentices should |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | can describe the main types of common attack techniques; also the role of human behaviour. Explain how attack techniques combine with motive and opportunity to become a threat. | 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.<br>• 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.<br>• 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.<br>• Describe typical hazards and how these may achieve the same outcome as an attack (e.g. flood, fire) | illustrate the main features of how they work and suggest where and when they may be effective.<br>• Current attack types may include:<br>o Phishing<br>o Social engineering<br>o Malware<br>o Network interception<br>• Blended techniques may include:<br>o Advanced persistent threat (APT)<br>o Denial of service (DoS and DDoS)<br>o Information theft and ransomware |
| | | | Describe the role of human behaviour in cyber security, including an ability to:<br>• Explain the term 'insider threat'<br>• 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. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | 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'. | Describe ways to defend against attack techniques by considering the different ways in which controls may be used; including:<br>• Deter, protect, detect and react<br>• Preventative, directive, detective and corrective<br>• Physical, procedural (people) and technical<br>• An attack chain |
| | Relevant laws and ethics – describe security standards, regulations and their consequences across at least two sectors; the role of criminal and other law; key relevant features of UK and international law. | • 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.<br>• Appreciate the role of criminal law, contract law and other sources of regulation.<br>• 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 appropriate and applicable cyber security standards, regulations and their consequences for at least two sectors, comparing their differences. Examples of sectors may include:<br>• Government<br>• Public sector<br>• Charitable<br>• Finance<br>• 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:<br>• Common Criteria<br>• PCI-DSS<br>• FIPS-140-2<br>• CESG Assisted products (CAPS)<br>• COBIT |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | • 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.<br>• Describe the implications of international laws and regulations that 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).<br>• Describe the legal responsibilities of system users and how these are communicated effectively. | Describe and explain the main features and implications of laws and regulations that affect organisations, systems and users in the UK. Key areas to consider are:<br>• The main UK laws that are relevant to cyber security issues, including legal requirements that affect individuals and organisations. Examples could include:<br>o The Computer Misuse Act<br>o The Data Protection Act (DPA)<br>o The Human Rights Act<br>• 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:<br>o The Digital Millennium Act<br>o International Traffic in Arms Regulations (ITAR)<br>o Harbor (Safe Harbor)<br>o The Patriot Act<br>o General Data Protection Regulations (GDPR)<br>o The Network and Information Security Directive (NIS)<br>• The legal responsibilities of system users and how these may be communicated effectively |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | • Describe by reference to at least 1 generally recognised and relevant professional body the ethical responsibilities of a cyber-security professional. | 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. |
| | 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 | Describe and know how to apply relevant techniques for horizon scanning and can:<br>• Recall, discover and explain the relative merits of at least three external sources of horizon scanning. These may include:<br>o Market trend reports<br>o Academic research papers<br>o Professional journals<br>o Hacker conferences<br>o Online<br>o Government sponsored sources; including, but not limited to: The National Cyber Security Centre (NCSC), CiSP and CertUK<br>• Describe and explain the value of using a diversity of sources<br>• Explain the horizon scanning technique, using current examples from sources relevant to cyber security in the UK<br>• Determine the reliability and trustworthiness of different sources. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | example. | Describe and explain the application of at least one technique to identify trends in research and illustrate with an example. |
| | Threat trends – can describe the significance of identified trends in cyber security and understand the value and risk of this analysis | • Describe the significance of some identified trends in cyber security and understand the value and risk of this analysis. | Describe and explain the significance of some identified trends in cyber security. |
| | | | Explain the value and risk of this analysis. |
| 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 | Describe data formats and protocols in current use. |
| | | | Explain features of network protocols in widespread use on the Internet. Including:<br>• HTTPS<br>• HTTP<br>• SMTP<br>• SNMP<br>• TCP<br>• UDP<br>• IP |
| | | | Identify network failure modes and reasons why networks 'hang'. |
| | | | Describe approaches to error control in a network. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | layered model (e.g. TCP/IP), including the physical and data link layer. (e.g. https, HTTP, SMTP, SNMP, TCP, IP, etc).<br>• 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.<br>• 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 features of the following layered network models:<br>• TCP/IP Reference Model<br>• OSI 7 Layer Model |
| | | | Compare the differences between the following physical layer categories and datalink layer protocols:<br>• Physical Layers (including, Wireless, Fibre, Wired)<br>• Data Link Layer (including, Ethernet [802.3], Wireless LAN [802.11], Bluetooth) |
| | | | Describe current network routing protocols in use; including:<br>• RIP/RIP2<br>• RIP-NG<br>• OSPF<br>• OSPFv2<br>• OSPFv3 |
| | | | Compare the differences between static and dynamic routing. |
| | | | Demonstrate the relationship between factors that affect network performance; including:<br>• Bandwidth<br>• Number of users<br>• Nature<br>• Contention |
| | | | Explain methods of improving network performance; such as: traffic shaping and architecture. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| 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 adaptable nature of threats. | • Describe what good practice in design is and how this may contribute to security. [Use/refer to: Trustworthy Software Initiative (TSI) training material].<br>• 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).<br>• 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. | 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, such as:<br>• Least privilege<br>• Economy of mechanism<br>• Defence in depth (complete mediation)<br>• Human factors - psychological acceptability<br>• Fail-safe defaults<br>• Open design<br>• Separation of privileges<br>• Least common mechanism |
| | | | Explain the following features of the Trustworthy Software Initiative (TSI):<br>• Safety<br>• Reliability<br>• Availability<br>• Resilience<br>• Security |
| | | | Understand TSI and IT Security Design Principles and explain their commonalities. |
| | | | Demonstrate the difference between enterprise architecture and security architecture, and explain where their physical and logical boundaries may exist. |
| | | | Describe the features of common frameworks for security architectures such as:<br>• SABSA<br>• Zachman Framework<br>• TOGAF |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | | • ITIL<br>• CoBIT<br>• The NIST Cyber Security Framework |
| | | | Relate how national bodies such as NCSC, GCHQ, NIST and FIPS provideguidance and information to public and private sector organisations in the following areas:<br>• IT Security policies<br>• IT Security architectural patterns / frameworks<br>• White papers<br>• National strategies on cyber security |
| | | | Understand the purpose and features of the Common Criteria evaluation model,such as:<br>• Common Criteria – their application and uses<br>• Target of Evaluation (TOE)<br>• Protection Profile<br>• Security Target<br>• EALs<br>• 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. |
| | | | Describe the properties of a Security Case for a known system, including:<br>• A clear definition of the security objectives of the case: who, what,where, why and when<br>• Threats that are likely to exist against the target system such as; physical, intrusion, malware |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | | • Risks to the system, measured in probabilities (very likely, likely and unlikely)<br>• Potential impact / severity (major, moderate, minor)<br>• Strategies for dealing with risks (avoid, accept, mitigate, transfer)<br>• Physical protection measures that may be required; for example:<br>• CCTV / alarms<br>  o Access control e.g. biometric<br>  o Fire suppression<br>  o Backups<br>  o Cabinets |
| | | | Interpret, describe and explain the security measures that should appear within a Security Case:<br>• Technical protection measures using hardware devices; such as:<br>  o Firewalls<br>• Routers Software components; such as:<br>  o Access rights<br>  o Anti-virus<br>  o Scanners<br>  o SIEM<br>• Implementation strategies for a proposed solution; such as:<br>  o Constraints<br>  o Dependencies<br>  o Cost benefit analysis |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | | • IT security policies that may be needed as part of the security case; such as: backups and data protection.<br>• System testing including the test plan, descriptors, test selection analysis and test results. |
| | | | Considering the Security Case, describe and explain:<br>• Applicable processes that may need to be implemented by personnel or systems<br>• Overview of legal responsibilities, where applicable<br>• Staff training that maybe required for the new measures<br>• Future proofing<br>• Alternative solutions to the case for due consideration, for example:<br>o OTS solutions<br>o Third-party contracts<br>o Complete software solutions |
| | | | Describe how threats evolve over time to respond to system security hardening. |
| 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: | • 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 | Describe computer and data authentication methods in current use. |
| | | | Describe methods employed to protect and secure data held on the host.<br>• types of authentication;<br>• access control;<br>• physical security;<br>• TCP ports; |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | hardware and software. | 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. | • disk encryption;<br>• checksums. |
| | | | Explain the importance of and the methods employed to keep the software environment healthy and up to date.<br>• Zero-day attacks;<br>• operating system and application updates;<br>• antivirus updates. |
| | | | Describe the responsibilities of the user for PC protection, in keeping their PC and its data secure from threats.<br>• social engineering;<br>• software updates;<br>• password management;<br>• internet etiquette. |
| | | | Describe the hardware components available for network protection and their purpose and identify the appropriate system for a given task.<br>• firewalls and DPI;<br>• application proxies;<br>• IDS vs. IPS;<br>• RADIUS;<br>• AAA. |
| | | | Describe the policy based methods available for network protection and explain their purpose.<br>• QoS;<br>• cross-domain components;<br>• DMZ;<br>• gateways;<br>• routing; |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria<br>The Learner Can… |
|---|---|---|---|
| | | | • traffic prioritisation;<br>• 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. Secure Internet transaction technologies include:<br>• IPSec;<br>• TLS;<br>• SSH;<br>• negotiation;<br>• cryptography;<br>• 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 well as available methods.<br>• network segregation;<br>• security issues for common client and server configuration;<br>• performance management;<br>• staff training;<br>• file and user permissions;<br>• password management. |
| | | | Describe frameworks and processes available for secure application development and apply appropriate |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | | security processes to the software development lifecycle.<br>• OWASP Top 10 awareness for web application development;<br>• Common Weakness Enumeration guideline awareness for general software development;<br>• National Cyber Security Centre (NCSC) guidelines;<br>• Secure SDLC. |
| | | | Describe IDAM Tools and systems available for application and data protection, and how these can be applied to manage application security.<br>• identity management systems and protocols;<br>• tickets;<br>• tokens;<br>• session;<br>• multi factor authentication;<br>• access control;<br>• 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. Indicative technologies can include:<br>• application sensors;<br>• application firewalls;<br>• proxies and reverse proxies; |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | | • application level security logging and monitoring;<br>• 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.<br>• Field vs record based encryption;<br>• SQL security;<br>• backup security;<br>• database access control. |
| | | | Correctly apply risk mitigation techniques:<br>• Threat modelling (STRIDE);<br>• 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.<br>• confidentiality (select layers for encryption);<br>• integrity (validating the integrity of data transmissions);<br>• availability (load balancing, proxies, anti DDOS, WAF). |
| | | | Explain accreditation and assurance processes that relate to the application of security technology. Apprentices will demonstrate the ability to apply supplier, software and component assurance and accreditation processes(first introduced in the Cyber |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | | Security Technologist, Knowledge Module 2 and described in sections 1 to 3 above).<br>• penetration testing;<br>• vulnerability assessment and threat intelligence;<br>• Information Security Management System (ISMS) and standards role in accreditation and supplier assurance (ISO27001, Payment Card Industry Data Security Standard (PCI DSS), common criteria, product assurance);<br>• software code review such as:<br>o SAST (Static Application Security Testing);<br>o DAST (Dynamic Application Security Testing);<br>o IAST (Interactive Application Security Testing). |
| | | | Describe Security Technology Solutions in terms of their benefits and limitationsand explain strengths, weakness and applicability of security technology as described in section 1 to 3 above.<br>• automation vs. manual validation of security;<br>• open source vs. closed source solutions;<br>• on premises vs. off premises solutions:<br>o cloud based;<br>o private;<br>o hybrid;<br>o public.<br>• iterative vs. Waterfall projects implication on security engineering. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| BCS Level 4 Certificate in Employment of Cryptography | Understands the basics of cryptography – can describe the main techniques, the significance of key management, appreciate the legal issues. | • 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).<br>• Explain the significance of key management and the main features, benefits and limitations of symmetric and public key cryptosystems and the significance of entropy.<br>• 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. | Describe cryptographic techniques and state their limitations.<br>• Ciphers;<br>• asymmetric (public key) and Symmetric;<br>• digital signatures;<br>• hashing;<br>• block cipher. |
| | | | Describe the main features of asymmetric (public key) and symmetric cryptosystems, and key exchange. |
| | | | Show where the various cryptographic techniques may be employed to secure data and systems.<br>• password verification;<br>• digital signatures;<br>• Virtual Private Networks (VPNs);<br>• tunnelling;<br>• encapsulating and carrier protocols;<br>• IPsec. |
| | | | Show how poorly applied cryptography can become a threat vector:<br>• ECB mode;<br>• collision attacks;<br>• algorithm problems;<br>• key management problems. |
| | | | Explain the significance and role of entropy in cryptography and discuss security problems associated with entropy. |
| | | | Explain the significance of key management as it relates to controls, lifecycle and governance. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria The Learner Can… |
|---|---|---|---|
| | | • 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 the role of cryptography in a range of common public systems:<br>• GSM;<br>• Chip and PIN;<br>• common hard disk encryption;<br>• TLS;<br>• SSL;<br>• privacy enforcing technology. |
| | | | Describe the role of cryptography as it applies to data on hard disks or in transit:<br>• secure Internet transaction technologies;<br>• data at rest;<br>• open vs closed source. |
| | | | List some of the practical issues encountered in implementing cryptography. Indicative areas include:<br>• performance considerations;<br>• storage of keys;<br>• security clearance of custodians;<br>• historical consideration of broken cryptographic systems;<br>• theoretical vs practical security;<br>• Kerckhoff's principle. |
| | | | Explain the practical issues faced when updating cryptographic techniques:<br>• vulnerability analysis;<br>• intelligence sources;<br>• general understanding of validation processes;<br>• patching process and testing. |

| Qualification Name | IFA Knowledge Standard | Occupational Brief Expected Minimum Requirement | Assessment Criteria<br>The Learner Can… |
|---|---|---|---|
| | | | List the regulatory frameworks in place in different jurisdictions, covering such topics as:<br>• International Traffic in Arms Regulations (ITAR);<br>• DPA;<br>• FoI;<br>• The Combined Code;<br>• Sarbanes-Oxley and their areas of governance;<br>• RIPA 2000;<br>• Key escrow;<br>• International Data Encryption Algorithm (IDEA). |
| | | | Identify the legal issues related to cryptography with respect to national borders understand key length and algorithms outlined in the Export Administration Regulations (EAR). |
| | | | List a range of resources available to obtain advice concerning cryptography and security:<br>• CAVP;<br>• CVE lists;<br>• open vs. closed reviews;<br>• ISO;<br>• OWASP;<br>• SANS;<br>• NIST;<br>• NCSC. |

## 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:<br>• Discover (through a mix of research and practical exploration) vulnerabilities in a system.<br>• 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.<br>• 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).<br>• 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:<br>• 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.<br>• 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:<br>• Identify and follow organisational policies and standards for information and cyber security.<br>• 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:<br>• 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.<br>• 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:<br>• 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.<br>• 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:<br>• 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.<br>• Select and configure at least 2 types of common security hardware and software components to implement a given security policy.<br>• 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.<br><br>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).<br><br>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.<br>Are aware of their own strengths in the job role, and any areas for improvement.<br>Appreciate who else is important, for them to do their job and fulfil the role effectively (e.g. colleagues, managers, other stakeholders).<br>Are aware of potential risks in the job role (e.g. security, privacy, regulatory).<br>Use personal attributes effectively in the role.<br>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.<br>Aware of the commercial objectives of the tasks/ projects they are working on.<br>Understands their role in meeting or exceeding customers' requirements and expectations.<br>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:<br>• Recognises the conclusion to be reached;<br>• Proceeds by rational steps;<br>• Evaluates information, judging its relevance and value;<br>• Supports conclusions, using reasoned arguments and evidence.<br>Creative thinking:<br>• Explores ideas and possibilities;<br>• Makes connections between different aspects;<br>• 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:<br>• Analyses situations;<br>• Defines goals;<br>• Contributes to the development of solutions;<br>• Prioritises actions;<br>• 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.<br><br>Apprentices can establish and maintain productive working relationships, and can use a range of different techniques for doing so. | Managing relationships:<br>• Understands the value and importance of good relationships;<br>• Acknowledges other people's accomplishments and strengths;<br>• Understands how to deal with conflict;<br>• Promotes teamwork by participating;<br>Customer / client relationships:<br>• Understands their requirements, including constraints and limiting factors;<br>• Sets reasonable expectations;<br>• Understands how to communicate with them in decisions and actions;<br>• Interacts positively with them;<br>• Provides a complete answer in response to queries ('transparency', 'full disclosure')<br>Stakeholders:<br>• Understands who they are and what their 'stake' is;<br>• Prioritises stakeholders in terms of their importance, power to affect the task and interest in it;<br>• 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.<br><br>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:<br>• Understands the purpose of communicating in a particular situation or circumstance (e.g. inform, instruct, suggest, discuss, negotiate etc.);<br>• Checks that the person/people with whom one is communicating also understand the purpose;<br>• Is sensitive to the dynamics of the situation;<br>• Is aware of anything that might disrupt the effectiveness of the communication (e.g. status, past history);<br>Method:<br>• Understands the most appropriate method for the situation;<br>• Aware of the limitations of the chosen method, and the possible risks of miscommunication (e.g. ambiguity);<br>• Takes account of the affective dimensions of the method (e.g. body language, tone of voice, eye contact, facial expression etc.);<br>Execution:<br>• Expresses self clearly and succinctly, but not over-simplifying;<br>• Checks that the other person/people understand what is being expressed;<br>• Takes account of the potential barriers to understanding (e.g. filtering, selective perception, information overload);<br>• 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.<br><br>Takes the initiative in identifying and negotiating appropriate personal development opportunities.<br><br>Demonstrates effective communication skills.<br><br>Contributes fully to the work of teams.<br><br>Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures.<br><br>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.<br><br>Applies a methodical approach to issue definition and resolution.<br><br>Undertakes all work in accordance with agreed safety, technical and quality standards, using appropriate methods and tools. |
| Influence | Interacts with and influences colleagues.<br><br>Has working level contact with customers, suppliers and partners.<br><br>May supervise others or make decisions which impact the work assigned to individuals or phases of projects.<br><br>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.<br><br>Uses discretion in identifying and responding to complex issues and assignments.<br><br>Usually receives specific instructions and has work reviewed at frequent milestones.<br><br>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.<br><br>Undertakes work that is more complex, more critical or more difficult.<br><br>Demonstrates an ability to extend or enhance their approach to work and the quality of outcomes.<br><br>Doesn't just solve the problem but explores all known options to do it better, more efficiently, more elegantly or better meet customer needs.<br><br>Shows good project management skills, in defining problem, identifying solutions and making them happen. |
| Complexity | Demonstrates a disciplined approach to execution, harnessing resources effectively.<br><br>Drives solutions – with strong goal focused and appropriate level of urgency. |
| Influence | Externally – works with customers, suppliers, and partners in a variety of situations.<br><br>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.<br><br>Reads situation, adapts behaviours, and communicates appropriately for the situation and the audience.<br><br>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 so there may be a small number of areas within these mandatory requirements that are not naturally occurring within the day-to-day duties of the apprentice. If it is not possible for the apprentice to demonstrate competence within their duties, a synoptic project should be selected that will allow the apprentice to demonstrate that they are competent in criteria that they are not exposed to during their normal working activities.

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 so there may be a small number of areas within these mandatory requirements that are not naturally occurring within the day-to-day duties of the apprentice. If it is not possible for the apprentice to demonstrate competence within their summative portfolio, a synoptic project should be selected that will allow the apprentice to demonstrate that they are competent in criteria that they are not exposed to during their normal working activities.

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.<br><br>Gaining knowledge of IT activities in the employing organisation external to their function. | • organisation charts;<br>• company annual reports;<br>• company website;<br>• 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.<br><br>Undertaking learning and practice in oral and written communications, including report writing and presentations.<br><br>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;<br>• 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.<br><br>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;<br>• 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.<br><br>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;<br>• 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;<br>• written evidence summarising learning gained from reading. |