Digital Industries Apprenticeship: Occupational Brief

Cyber Security Technologist

April 2016

Digital Industries Apprenticeships: Occupational Brief

Level 4 Cyber Security Technologist Apprenticeship

Minimum Standards and Grading Criteria

This paper defines the minimum requirements for the knowledge, skills and behaviours defined in the standard, which are required for a pass. It also defines the criteria to be used for awarding the grade for merit or distinction. This paper should be read in conjunction with the Standard and Assessment Plan for the Level 4 Cyber Security Technologist Apprenticeship

Overview of Grading

There are three sets of criteria on which the assessment and grading is made. The three criteria are

The What: what the apprentice has shown they can do,

The How: the way in which the work has been done

The With Whom: The personal and interpersonal qualities the apprentice has brought to all their work relationships

Each of these three criteria has minimum (expected) requirements, which must be satisfied for a pass.

Each of these criteria has a number of dimensions which should be considered to determine if the apprentice is significantly above the minimum (expected) level of quality

The purpose of grading is to differentiate between those apprentices whose work is at the expected level of quality against the totality of the skills, knowledge and behaviours specified in the standard and those whose work is significantly above this expected level

For a pass, each of the three sets of criteria must demonstrate at least the expected (minimum requirement) level of quality

For a merit, the What has to be significantly above the level of quality and one of either the How or the With Whom has to be significantly above the level of quality expected

For a distinction, each of the three sets of criteria must be significantly above the expected level of quality

The assessor takes a holistic judgement of whether or not their assessments demonstrate that the apprentice is "significantly above the expected level of quality" in each of these three areas and can then determine which grade should be awarded

The what – what the apprentice has shown they can do

Minimum Requirements

The following table shows what the minimum, expected requirements are for a pass on this criteria

CORE

Competency Standard	**Minimum, expected, requirements for a pass**
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.

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).
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.
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.

OPTION 1: TECHNOLOGIST

Competency Standard	**Minimum, expected, requirements for a pass**
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.
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.
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.

OPTION 2: RISK ANALYST

Competency Standard	**Minimum, expected, requirements for a pass**
Make cyber security risk assessments	The apprentice should be able to: • Conduct a cyber-risk assessment against an externally (market) recognised cyber security standard using a recognised risk assessment methodology. • Identify threats relevant to a specific organisation and/or sector.
Develop security policy and processes	The apprentice should be able to: • Develop an information security policy or process to address an identified risk. • Develop an information security policy within a defined scope to take account of a minimum of 1 law or regulation relevant to cyber security.
Provide audit and assurance	The apprentice should be able to take an active part in a security audit against a recognised cyber security standard, undertake a gap analysis and make recommendations for remediation.
Develop incident response and business continuity plans	The apprentice should be able to: • Develop an incident response plan for approval (within an organisations governance arrangements for incident response). • Develop a business continuity plan for approval (within an organisations governance arrangements for business continuity).
Improve the cyber security culture in an organisation	The apprentice should be able to: • Assess security culture using a recognised approach. • Design and implement a simple ‘security awareness’ campaign to address a specific aspect of a security culture.

The What – what the apprentice has shown they can do

Criteria for a Merit or Distinction

The following table shows what the apprentices would need to demonstrate to be assessed as significantly above the expected level for what they have done

Dimensions	**Description of what significantly above the expected level of quality looks like**
Breadth – the range of tools and methods understand and applied	Understands and applies a wide range of tools and methods Accurately and appropriately applies and effectively implements the right tools and methods in a variety of different situations
Depth – the level to which these tools and methods are understood and applied	A capable user - exploits the functionality/capability of the tools and methods Broad understanding of different tools and methods and how and why they can be applied in different contexts
Complexity – the extent and prevalence of inter-related and inter-dependant factors in the work and how well the apprentice has dealt with these	Deals confidently and capably with interrelated and interdependent factors in their work

The how: the way in which the work has been done

The following table shows what the minimum, expected requirements are for a pass on this criteria

Competency Standard	Minimum expected requirements for a pass
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
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

The How: the way in which the work has been done

Criteria for a Merit or Distinction

The following table shows what the apprentices would need to demonstrate to be assessed as significantly above the expected level for the way in which the work has been done

Dimensions	Description of what significantly above the expected level of quality looks like
Responsibility – the scope of responsibility and level of accountability demonstrated in the apprentices work	Undertakes work that is more complex, more critical or more difficult Works independently and takes responsibility
Initiative	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 to better meet customer needs
Delivery focus – the extent to which the apprentice has shown they can grasp the problems, identify solutions and make them happen to meet client needs	Shows good project management skills, in defining problem, identifying solutions and making them happen Demonstrates a disciplined approach to execution, harnessing resources effectively Drives solutions – with a strong goal focused and appropriate level of urgency

The with whom: the personal and interpersonal qualities the apprentice has brought to internal and external relationships

Minimum Requirements

The following table shows what the minimum, expected requirements are for a pass on this criteria

	Minimum expected requirements for a pass
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 • Undersands 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
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.	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)

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.	a. 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.) b. 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

The With Whom: the personal and interpersonal qualities the apprentice has brought to internal and external relationships

Criteria for Merit or Distinction

The following table shows what the apprentices would need to demonstrate to be assessed as significantly above the expected level for the personal and interpersonal qualities the apprentice has brought to internal and external relationships

Dimensions	**Description of what significantly above the expected level of quality looks like**
Scope and appropriateness – the range of internal and external people and situations that the apprentice has	Internally – works alone, 1:1, in a team and with colleagues at all levels

engaged appropriately and effectively with	Externally – works with customers, suppliers and partners in a variety of situations Reads situations, adapts behaviours, and communicates appropriately for the situation and the audience
Reliability – the extent to which they perform and behave professionally	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
A role model and exemplar to others	Actively works with others and leads by example

Annex: Cyber Security Technologist / Risk Analyst: Knowledge and Understanding

Knowledge and Understanding is assessed on programme through Knowledge Modules.

Knowledge Module 1 (this is the Core, so ALL the apprentices take this module): Cyber Security Introduction

The Knowledge Standards	Definition of the Minimum Requirements
Foundation *This module is a specialist knowledge base application to cyber security. It contains essential knowledge foundations for the majority of cyber security roles.*	Why cyber security matters • Explain why information and cyber security is important to business and society. Basic security theory • Explain basic concepts: security, identity, confidentiality, integrity, availability, threat, vulnerability, risk & 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 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 cyber-security risk assessment, taking account the wider business risk context Security assurance • Assurance concepts: Explain the difference between 'trusted' and 'trustworthy' and explain what assurance is for in security. Describe the main approaches to assurance (intrinsic, extrinsic, design & 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 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. Applying basic security concepts to develop security requirements (to help build a security case) • Derive and justify security objectives. Describe how these might apply to information and infrastructure assets in at least 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. Security concepts applied to ICT ('cyber') infrastructure • Describe some common vulnerabilities in computer networks and systems (for example, non-secure coding and unprotected networks) • Describe the fundamental building blocks (e.g. routers, switches, hubs, storage, transmission) and typical architectures (e.g. server/client, hub/spoke, non-virtual/virtual) of computers, networks and the Internet. Attack techniques and common sources of threat • Describe the main different types of common attack techniques (for example: phishing, social engineering, malware, network interception, blended techniques e.g. 'advanced persistent threat', denial of service, theft). Explain the main features of how they work and suggest where they may be effective. • Describe the role of human behaviour in cyber security. Explain what 'the insider threat' is. Explain what 'cyber security culture' in an organisation is, describe some features that may characterise it and explain how it may contribute to security risk. • Explain how an attack technique combines with motive and opportunity to become a threat. Explain how attack techniques are developed and why they are continuously changing. • Describe typical hazards and how these may achieve the same outcome as an attack (e.g. flood, fire)

Cyber defence

- Describe ways to defend against the main attack techniques, including consideration of ‘deter’, ‘protect’, ‘detect’ & ‘react’ and an ‘attack chain’.

Legal, standards, regulations and ethical standards relevant to cyber security

- Describe the cyber security standards and regulations and their consequences for at least 2 sectors (e.g. Government, finance, petrochemical/process control), comparing and contrasting the differences.
- Appreciate the role of criminal law, contract law and other sources of regulation.
- Explain the benefits & 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 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.

Keeping up with the threat landscape

- Describe and know how to apply at relevant techniques for horizon scanning and be able to identify at least three external sources of horizon scanning (e.g. market trend reports, academic research papers, professional journals, hacker conferences, 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.

Future trends

Describe the significance of some identified trends in cyber security and understand the value and risk of this analysis

No Vendor or Professional Certifications have been identified that would exempt apprentices from this Knowledge Module

Modules 2 – 5 below are for Option 1: Technologist

Knowledge Module 2: Network and Digital Communications Theory

The Knowledge Standards	**Definition of the Minimum Requirements**
Networks *This is a general introduction to modern computer networks and not specific to cyber security.*	• Explain what is meant by data and protocol and how they relate to each other. Describe an example data format and a simple protocol in current use (using protocol diagrams). Describe example failure modes in protocols, for example reasons why a protocol may 'hang' and the effect on a protocol of data communication errors, Describe at least one approach to error control in a network. Describe the main features of network protocols in widespread use on the Internet, their purpose and relationship to each other in a layered model (e.g. TCP/IP), including the physical and data link layer. (e.g. https, HTTP, SMTP, SNMP, TCP, IP, etc). • Describe the main routing protocols in current use in computer networks and explain the differences between static and dynamic routing protocols and the pros and cons of each in different circumstances. • Explain some of 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).

No Vendor or Professional Certifications have been identified that would exempt apprentices from this Knowledge Module

Knowledge Module 3: Security Case Development and Design Good Practice

The Knowledge Standards	Definition of the Minimum Requirements
Security cases *This builds on "Applying basic security concepts to develop security requirements (to help build a security case)" in KM1 and is an advanced module focused on security case development.*	• Describe what good practice in design is and how this may contribute to security. [Use/refer to: Trustworthy Software Initiative (TSI) training material]. • Describe common security architectures that incorporate security hardware and software components. Be aware of sources of reputable security architectural patterns and guidance (e.g. vendor or Government). • Understand how to develop a 'security case'. (A security case, sometimes also called a security target' describes the context, security objectives, threats, and for every identified attack technique identify a mitigation/security controls – technical, implementation or policy/process), recognizing that threats evolve and threats also respond to a security design.

No Vendor or Professional Certifications have been identified that would exempt apprentices from this Knowledge Module

Knowledge Module 4: Security Technology Building Blocks

The Knowledge Standards	**Definition of the Minimum Requirements**
Building blocks *This is all about cyber security technology components typically deployed in networks & systems to provide security functionality*	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 options) of the component, describing any residual risks.

No Vendor or Professional Certifications have been identified that would exempt apprentices from this Knowledge Module

Knowledge Module 5: Employment of Cryptography

The Knowledge Standards	**Definition of the Minimum Requirements**
Cryptography *This is applied cryptography.*	• Describe the main cryptographic techniques (e.g. symmetric, public key, secure hash, digital signing, block cipher etc), how they are applied and to what end and their limitations (including study of some examples of badly applied or implemented cryptographic techniques). • Explain the significance of key management and the main features, benefits and limitations of symmetric and public key cryptosystems and the significance of entropy.

	• Describe the role of cryptographic techniques in a range of different systems (e.g. GSM, Chip&PIN, common hard disk encryption, TLS, 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.

No Vendor or Professional Certifications have been identified that would exempt apprentices from this Knowledge Module

Modules 6 and 7 below are for Option 2: Risk Analyst

Knowledge Module 6: Risk Assessment

The Knowledge Standards	**Definition of the Minimum Requirements**
Risk assessment *This is about cyber risk assessment*	• Describe relevant risk assessment methodologies commonly used in the context of information security and know how to apply in practice. • Identify the vulnerabilities in organisations security management system. Identify the links between physical, logical, personal and procedural security. Describe how an employee may enable a successful attack chain without realising it. Describe some things that may increase or decrease risks related to an organisations 'cyber culture'. • Understand the threat intelligence lifecycle and the concepts of threat actors and attribution. • Describe different approaches to risk treatment (accept, transfer, avoid, mitigate) and management in practice with examples (which may be technical, business process, or other …). Understand the role of the risk owner and

	contrast the perspective of the risk owner with that of other stakeholders. Risks may be described in qualitative, quantitative terms or some combination thereof.

No Vendor or Professional Certifications have been identified that would exempt apprentices from this Knowledge Module

Knowledge Module 7: Governance, Organisation, Law, Regulation and Standards

The Knowledge Standards	**Definition of the Minimum Requirements**
Underpinning structure *This builds on the "Legal, standards, regulations and ethical standards relevant to cyber security" in KM1, focusing on information security management, data protection and privacy. It also covers governance and organisational issues that relate to cyber security and that are affected by cyber risk.*	Governance & organisation • Explain the need for appropriate governance, organisational structure, roles, policies, standards and guidelines for cyber and information security, and how they work together to deliver identified security outcomes. • Explain how an organisation's security policies, standards and governance are supported by provisioning and access rights (e.g. how identity and access management are implemented and maintained for a database, application or physical access control system). • Describe how cyber security policies and procedures are used in different organisational environments and affect individuals and organisations. • Understand the roles of experts in the cyber security industry, how they are recognised, and the work they do • Understand how to effectively use organisations such as a CERT, OSINT provider and incident response provider. Standards, law, regulation and information security management • Awareness of the legal framework surrounding intelligence gathering and the relationship to data protection, human rights and privacy.

	• Explain the key concepts and benefits of applying ISO27001 to implement an information security management system • Awareness of legal and regulatory obligations for breach notification.

No Vendor or Professional Certifications have been identified that would exempt apprentices from this Knowledge Module