BCS Level 4 Certificate in Cyber Security Introduction Syllabus QAN 603/0830/8

Version 1.2
November 2016

This is a United Kingdom government regulated qualification which is administered and approved by one or more of the following: Ofqual, Qualification in Wales, CCEA or SQA.

BCS Level 4 Certificate in Cyber Security Introduction Syllabus

Contents

Change History

Any changes made to the syllabus 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	Changes Made
Version 1.0 Nov 2016	Syllabus Created
Version 1.1 Nov 2016	Amended terminology for Harbour
Version 1.2 Nov 2016	Added mandatory Ofqual text

Introduction

This Certificate is the first of seven knowledge modules that are applicable to the Level 4 Cyber Security Technologist Apprenticeship. This is a general introduction to cyber security and is the core element of the apprenticeship. It covers the essential knowledge foundation for most cyber security roles.

Objectives

Apprentices should be able to demonstrate an understanding of the foundations of cyber security. Key areas are:

1. Describe and explain why information and cyber security are important to business and to society.
2. Recall, describe and explain the terminology and basic concepts of cyber security.
3. Demonstrate and explain the concept of information assurance and how it can be delivered.
4. Describe and explain how security objectives can be developed and used to build a security case.
5. Demonstrate and explain how the basic security concepts can be applied to typical information and communications technology (ICT) cyber infrastructures.
6. Describe and explain common attack techniques and sources of threat.
7. Illustrate and explain ways to defend against the main attack techniques.
8. Recall, describe and explain legal, regulatory, information security and ethical standards relevant to the cyber-community.
9. Discover and explain the concept and practice of keeping up with the threat landscape (horizon scanning).
10. Describe and explain future trends in cyber security.

Evidence of lessons learnt in these key areas should be collected and reflected upon when the Apprentice is compiling the Summative Portfolio as the apprentice could identify how the task might be done better/differently with knowledge subsequently gained.

Target Audience

The certificate is relevant to anyone requiring an understanding of the core principles and foundations of a Cyber Security Technologist.

Course Format and Duration

Apprentices can study for this certificate by attending a training course provided by a BCS accredited Training Provider. The estimated total qualification time for this certificate is 199 hours.

Eligibility for the Examination

There are no specific pre-requisites for entry to the examination; however, apprentices should possess the appropriate level of knowledge to fulfil the objective shown above. Individual employers will set the selection criteria, but this is likely to include A' Levels, a relevant Level 3 apprenticeship, or other relevant qualifications, relevant experience and/or an aptitude test with a focus on functional maths.

Duration and Format of the Examination

The format for the examination is a one-hour multiple-choice examination consisting of 40 questions. The examination is closed book (no materials can be taken into the examination room). The pass mark is 26/40 (65%).

Additional Time for Apprentices Requiring Reasonable Adjustments Due to a Disability

Apprentices may request additional time if they require reasonable adjustments. Please refer to the reasonable adjustments policy for detailed information on how and when to apply.

Additional Time for Apprentices Whose Language Is Not the Language of the Exam

If the examination is taken in a language that is not the apprentice's native/official language, then they are entitled to 25% extra time.

If the examination is taken in a language that is not the apprentice's native/official language, then they are entitled to use their own **paper** language dictionary (whose purpose is translation between the examination language and another national language) during the examination. Electronic versions of dictionaries will **not** be allowed into the examination room.

Guidelines for Accredited Training Organisations

Each major subject heading in this syllabus is assigned an allocated time. The purpose of this is two-fold: firstly, to give both guidance on the relative proportion of time to be allocated to each section of an accredited course and an approximate minimum time for the teaching of each section; secondly, to guide the proportion of questions in the exam. Accredited Training Organisations may spend more time than is indicated and apprentices may spend more time again in reading and research. Courses do not have to follow the same order as the syllabus. Courses may be run as a single module or broken down into two or three smaller modules.

This syllabus is structured into sections relating to major subject headings and numbered with a single digit section number. Each section is allocated a minimum contact time for presentation. Apprentices should be encouraged to consider their Summative Portfolio throughout the modules.

Syllabus

For each top-level area of the syllabus, a percentage and K level is identified. The percentage is the exam coverage of that area, and the K level identifies the maximum level of knowledge that may be examined for that area.

1. Why Cyber Security Matters (5%, K2)

In this key topic, the apprentice will describe and explain why information and cyber security are important to business and to society. Outcomes should include an ability to:

1.1 Describe and explain the evaluation of information assets and the criticality to a business.

1.2 Describe and explain how cyber security can have a direct impact on the reputation and continuing success of a business.

1.3 Describe and explain how the cyber security of businesses contributes to the overall economy and security of the society in which it operates.

2. Basic Security Theory (10%, K2)

In this key topic, the apprentice will recall, relate and explain the terminology and basic concepts of cyber security. Outcomes should include an ability to:

2.1 Recall and explain key terminology. This could include, but not be limited to:
- Security
- Identity
- Authentication
- Non-repudiation
- Confidentiality
- Integrity
- Availability
- Threat
- Vulnerability
- Risk and hazard

2.2 Describe what security is, fundamentally, by explaining:
- How the concepts of threat, hazard and vulnerability relate to each other and lead to risk.
- The inherent asymmetric nature of cyber security threats.

2.3 Describe and explain:
- What risk is
- How risks are usually quantified (by likelihood and relative impact)

- The use of at least one commonly used tool for risk management; for example, but not limited to, a risk register.

2.4 Describe typical threats, threat actors and hazards in terms of capability, opportunity and motive using examples that may concern an organisation. These may include, but not be limited to:
- Profiling techniques
- Relating these threat descriptions to example security objectives

2.5 Describe and explain how an organisation balances business drivers and costs with the outcome and recommendations of a cyber security risk assessment. Apprentices will also consider the wider business risk context using, as an example, but not limited to: a business impact assessment (BIA).

3. Security Assurance (10%, K3)

In this key topic, the apprentice should explain the concept of security assurance and demonstrate how it can be delivered. Outcomes should include an ability to:

3.1 Recall, describe and explain security assurance concepts and how these might be applied at different stages in the lifecycle of a system; including, but not limited to:
- The difference between 'trusted' and 'trustworthy'
- The purpose of security assurance
- The main approaches to:
  - Assurance
  - Intrinsic and extrinsic
  - Design and implementation
  - Operational policy & process

3.2 Describe and explain the way security assurance works in practice regarding the concepts.

3.3 Describe and explain what penetration testing is and how it contributes to security assurance; for example, but not limited to 'ethical hacking'. Apprentices will also show an understanding of the differences between internal and external penetration testing.

3.4 Describe at least one current system of extrinsic assurance, explaining the benefits and limitations. For example, but not limited to:
- Security testing
- Supply chain assurance
- Common criteria

3.5 Describe at least two ways an organisation can provide intrinsic assurance.

4. Applying Basic Security Concepts to Develop Security Requirements (10%, K2)

In this key topic, the apprentice will describe and explain how security objectives can be used to build a security case. Outcomes should include an ability to:

4.1 Explain how to develop and justify security objectives for a proposed business solution.

4.2 Describe how security objectives might be used to define information and infrastructure assets in representative business scenarios.

4.3 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.

4.4 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.

5. Security Concepts Applied to ICT Cyber Infrastructure (15%, K3)

In this key topic, the apprentice will demonstrate and explain how basic security concepts can be applied to typical information and communications technology (ICT) cyber infrastructures. Outcomes should include an ability to:

5.1 Show an understanding of common vulnerabilities in computer networks and systems. This may include, but not be limited to, non-secure coding and unprotected networks.

5.2 Describe the fundamental building blocks of:

- Infrastructure elements; including, but not limited to:
  - Firewalls
  - Routers
  - Switches
  - Hubs
  - Storage
  - Transmission.
- Typical architectures of computers, networks and the Internet; including, but not limited to:
  - Server/ client
  - Hub/spoke
  - Non-virtual/ virtual.

6. Attack Techniques and Common Sources of Threat (15%, K3)

In this key topic, the apprentice will explain and demonstrate an understanding of common attack techniques and sources of threat. Outcomes should include an ability to:

6.1 Describe and explain the main types of attack techniques. For each type of attack, apprentices should illustrate the main features of how they work and suggest where and when they may be effective.

- Current attack types may include, but not be limited to:
  - Phishing
  - Social engineering
  - Malware
  - Network interception
- Blended techniques may include, but not be limited to:
  - Advanced persistent threat (APT)
  - Denial of service (DoS and DDoS)
  - Information theft and ransomware.

6.2 Describe the role of human behaviour in cyber security, including an ability to:

- Explain the term 'insider threat'
- Explain an organisation's 'cyber security culture' and describe some features that may characterise it. Apprentices should also show an understanding of how this cyber security culture may contribute to security risk.

6.3 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.

6.4 Describe typical hazards and how these may achieve the same outcome as an attack. For example, but not limited to, flood and fire.

7. Cyber Defence (15%, K3)

In this key topic, the apprentice will describe, solve and explain ways to defend against the main attack techniques. Outcomes should include an ability to:

7.1 Describe ways to defend against attack techniques by considering the different ways in which controls may be used; including, but not limited to:

- Deter, protect, detect and react
- Preventative, directive, detective and corrective
- Physical, procedural (people) and technical
- An attack chain

8. Legal, Regulatory, Information Security and Ethical Standards Relevant to Cyber Security (10%, K2)

In this key topic, the apprentice will recall, describe and explain the legal, regulatory, information security and ethical standards relevant to the cyber community. Outcomes should include an ability to:

8.1 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, but not be limited to:

- Government
- Public sector
- Charitable
- Finance
- Petrochemical/ process control.

8.2 Describe and explain the role of criminal law, contract law and other related sources of legal and regulatory control.

8.3 Describe and explain the benefits, costs and main motives for the uptake of significant security standards; including, but not limited to:

- Common Criteria
- PCI-DSS
- FIPS-140-2
- CESG Assisted products (CAPS)
- COBIT

8.4 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:

- The main UK laws that are relevant to cyber security issues, including legal requirements that affect individuals and organisations. Examples could include, but not be limited to:
  - The Computer Misuse Act
  - The Data Protection Act (DPA)
  - The Human Rights Act
- The international laws and regulations that affect organisations, systems and users in the UK covering the movement of data and equipment across international borders and between jurisdictions; including, but not limited to:
  - The Digital Millennium Act
  - International Traffic in Arms Regulations (ITAR)
  - Harbour (Safe Harbour)
  - The Patriot Act
  - General Data Protection Regulations (GDPR)
  - The Network and Information Security Directive (NIS)
- The legal responsibilities of system users and how these may be communicated effectively.

8.5 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.

9. Keeping Up with The Threat Landscape (5%, K3)

In this key topic, the apprentice will discover and explain the concept and practice of keeping up with the threat landscape (horizon scanning). Outcomes should include an ability to:

9.1 Describe and know how to apply relevant techniques for horizon scanning and can:

- Recall, discover and explain the relative merits of at least three external sources of horizon scanning. These may include, but not be limited to:
  - Market trend reports
  - Academic research papers
  - Professional journals
  - Hacker conferences
  - Online
  - Government sponsored sources; including, but not limited to: The National Cyber Security Centre (NCSC), CiSP and CertUK
- Describe and explain the value of using a diversity of sources
- Explain the horizon scanning technique, using current examples from sources relevant to cyber security in the UK
- Determine the reliability and trustworthiness of different sources.

9.2 Describe and explain the application of at least one technique to identify trends in research and illustrate with an example.

10. Future Trends (5%, K2)

In this key topic, the apprentice will describe and explain future trends in cyber security. Outcomes should include an ability to:

10.1 Describe and explain the significance of some identified trends in cyber security.

10.2 Explain the value and risk of this analysis.

Levels of Knowledge / SFIA Levels

This course will provide apprentices with the levels of difficulty / knowledge skill highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge and SFIA levels are explained in on the website www.bcs.org/levels. The levels of knowledge above will enable apprentices to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

Level	Levels of Knowledge	Levels of Skill and Responsibility (SFIA)
K7		Set strategy, inspire and mobilise
K6	Evaluate	Initiate and influence
K5	Synthesise	Ensure and advise
K4	Analyse	Enable
K3	Apply	Apply
K2	Understand	Assist
K1	Remember	Follow

Question Weighting

Syllabus Area	Target number of questions
1. Why Cyber Security Matters. (5%, K2)	2
2. Basic Security Theory. (10%, K2)	4
3. Security Assurance. (10%, K3)	4
4. Applying Basic Security Concepts to Develop Security Requirements. (10%, K2)	4
5. Security Concepts Applied to ICT 'Cyber' Infrastructure. (15%, K3)	6
6. Attack Techniques and Common Sources of Threat. (15%, K3)	6
7. Cyber Defence. (15%, K3)	6
8. Legal, Regulatory, Information Security and Ethical Standards Relevant to Cyber Security. (10%, K2)	4
9. Keeping Up with The Threat Landscape. (5%, K3)	2
10. Future Trends. (5%, K2)	2
Total	**40 Questions**

Format of Examination

Type	40 Question Multiple Choice.
Duration	1 Hour. An additional 15 minutes will be allowed for apprentices sitting the examination in a language that is not their native /mother tongue.
Pre-requisites	Accredited training is strongly recommended but is not a pre-requisite.
Supervised	Yes.
Open Book	No.
Pass Mark	26/40 (65%).
Calculators	Calculators cannot be used during this examination.
Total Qualification Time (TQT)	199 Hours.
Delivery	Online.

Trainer Criteria

Criteria	▪ Have 10 days' training experience or have a Train the Trainer qualification ▪ Have a minimum of 3 years' practical experience in the subject area

Classroom Size

Trainer to apprentice ratio	1:16

Recommended Reading List

Title: Information Security Management Principles
Author: Taylor, A. *et al.*
Publisher: BCS, The Chartered Institute for IT; 2nd edition
Publication Date: 18 Jun 2013
ISBN-13: 978-1780171753

Title: Information Risk Management: A practitioner's guide
Author: Sutton, D.
Publisher: BCS, The Chartered Institute for IT
Publication Date: 26 NOV 2014
ISBN-13: 978-1780172651