BCS Level 4 Certificate in Security Case Development and Design Good Practice Syllabus QAN 603/0904/0

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 Security Case Development and Design Good Practice 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	Added mandatory Ofqual text
Version 1.2 February 2017	Amendment to text colour on first page

Introduction

This Certificate is the third of seven knowledge modules that are applicable to the Level 4 Cyber Security Technologist Apprenticeship. This module builds on **Applying basic security concepts to develop security requirements (to help build a security case),** found in Knowledge Module 1 of the Cyber Security Technologist Apprenticeship and it is an advanced module focused on security case development.

Objectives

Apprentices should be able to demonstrate an understanding of modern cyber security design practice and devising a security case for a given system. Outcomes should include:

1. Describe what good practice in design is and how this may contribute to security.
2. Compare and contrast the features of reputable security architectures which incorporate security hardware and software components.
3. Describe the features of the Common Criteria Protection Profile.
4. Understand how to design and develop a 'security case', recognising that threats evolve and respond to a security design.

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 enrolled in the Level 4 Cyber Security Technologist apprenticeship programme requiring an understanding of good Design and Security Case Development as they relate to Cyber Security.

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 132 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 objectives 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; 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. IT Security Design Principles (20%, K3)

In this key topic, the apprentice will be able to describe and explain recognised IT Security Design Principles and demonstrate their application within IT systems and software. Outcomes should include an ability to:

1.1 Demonstrate the importance of keeping IT systems simple, whilst meeting business and security needs.

1.2 Describe the application and features of core IT Security Design Principles, including but not limited to:

- Least privilege
- Economy of mechanism
- Defence in depth (complete mediation)
- Human factors - psychological acceptability
- Fail-safe defaults
- Open design
- Separation of privileges
- Least common mechanism

1.3 Explain the following features of the Trustworthy Software Initiative (TSI):

- Safety
- Reliability
- Availability
- Resilience
- Security

1.4 Compare TSI and IT Security Design Principles and explain their commonalities.

2. Common Security Architectures (30%, K3)

In this key topic, the apprentice will be able to describe and illustrate common security architectures that incorporate hardware and software components. Outcomes should include an ability to:

2.1 Demonstrate the difference between enterprise architecture and security architecture, and explain where their physical and logical boundaries may exist.

2.2 Compare features of common security architectures; including, but not limited to:
- SABSA
- Zachman Framework
- TOGAF
- CISCO and the NIST Cyber Security Framework

2.3 Relate how national bodies such as CESG, FIPS, NIST and GCHQ provide guidance and information to public and private sector organisations in the following areas:
- IT Security policies
- IT Security architectural patterns/ frameworks
- White papers
- National strategies on cyber security

3. Common Criteria Protection Profile (20%, K2)

In this key topic, the apprentice will describe and explain the Common Criteria Protection Profile for a security component. Outcomes should include an ability to:

3.1 Explain the purpose and features of the Common Criteria evaluation model, including and not limited to:
- Common criteria – their application and uses
- Target of Evaluation (TOE)
- Protection profile
- Security target
- EALs
- The process of specification, implementation and evaluation for certified products and systems

3.2 Describe how Common Criteria may be used to feed into a security case.

4. Security Case (30%, K3)

In this key topic, the apprentice will construct a Security Case for a system. Outcomes should include an ability to:

4.1 Produce a Security Case for a known system, including:

- A clear definition of the objectives of the case: who, what, where, why and when
- Threats that are likely to exist against the target system
- Known attack profiles likely to be used by malicious individuals
- Risks to the system, measured in probabilities (very likely, likely and unlikely)
- Potential impact (major, moderate, minor)
- Potential severity (high, medium, low)
- Physical protection measures that may be required; for example, but not limited to:
  - CCTV/ alarms
  - Backups
  - Cabinets

4.2 Considering the Security Case, interpret what security measures should apply:

- Technical protection measures using hardware devices; including, but not limited to:
  - Firewalls
  - Routers
  - SIEM
- Software components; including, but not limited to:
  - Access rights
  - Anti-virus
  - Scanners
- Implementation strategies for a proposed solution; including, but not limited to:
  - Constraints
  - Dependencies
  - Cost benefit analysis
- IT security policies that may be needed as part of the security case; including, but not limited to: backups and data protection
- Where applicable, complete a test plan to include descriptors and expected results

4.3 Considering the Security Case, indicate examples of:

- Applicable processes that may need to be implemented by personnel or systems
- Overview of legal responsibilities, where applicable
- Staff training that maybe required for the new measures
- Future proofing
- Alternative solutions to the case for due consideration. For example, but not limited to:
  - OTS solutions
  - Third-party contracts
  - Complete software solutions

4.4 Describe (using software applications, hardware components and examples), how threats evolve over time to respond to system security hardening.

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. IT Security Design Principles. (20%, K3)	8
2. Common Security Architectures. (30%, K3)	12
3. Common Criteria Protection Profile. (20%, K2)	8
4. Security Case. (30%, K3)	12
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.
Learning Hours	132 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