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

Version 3.0
February 2020

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

Introduction 4

Objectives 4

Course Format and Duration 4

Eligibility for the Examination 4

Duration and Format of the Examination 5

Additional Time for Apprentices Requiring Reasonable Adjustments Due to a Disability 5

Additional Time for Apprentices Whose Language Is Not the Language of the Exam 5

Guidelines for Accredited Training Organisations 5

Syllabus 6

Levels of Knowledge / SFIA Levels 9

Question Weighting 9

Format of Examination 9

Trainer Criteria 10

Classroom Size 10

Recommended Reading List 10

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
Version 2.0 October 2019	Update to Question Weighting Removed "such as" and "including" from all learning outcomes.
Version 3.0 February 2020	Full syllabus review

Introduction

This certificate is the third of five knowledge modules that are applicable to the Technologist pathway for 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. 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).
3. Understand how to develop a 'security case', recognising that threats evolve, and threats also 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. Design Good Practice (27.5%, K2)

In this key topic, the apprentice will describe what good practice in design is and how this may contribute to security. Outcomes should include an ability to:

1.1 Describe the features of good systems design and explain how these contributes to security:

- OWASP Security by Design Principles:
  - minimize attack surface area;
  - establish secure defaults;
  - principle of least privilege;
  - principle of defence in depth;
  - fail securely;
  - don't trust services;
  - separation of duties;
  - avoid security by obscurity;
  - keep security simple;
  - fix security issues correctly.

1.2 Describe the facets of software trustworthiness as defined by The Trustworthy Software Framework and explain how each can be explicitly and implicitly assessed against an organisation's security requirements:

- safety;
- reliability;
- availability;
- resilience;
- security.

1.3 Explain the four levels of trustworthiness, how the control sets apply and explain under what circumstances each might be appropriate:

- TL1 Essential Practices;
- TL2 Assessed Practices;
- TL3 Enhanced Practices;
- TL4 Specialist Practices.

2. Security Architectures (30%, K2)

In this key topic, the apprentice will describe common security architectures that incorporate security hardware and software components and be aware of sources of reputable security architectural patterns and guidance. Outcomes should include an ability to:

2.1 Explain the purpose and nature of security architecture and how it differs from enterprise architecture considering all the technology, people and processes relating to a computer system.

- NCSC secure design principles:
  - establish the context;
  - making compromise difficult;
  - making disruption difficult;
  - making compromise detection easier;
  - reducing the impact of compromise.

2.2 Explain the common security architecture frameworks in use.

- TOGAF;
- MODAF;
- Zachman;
- SABSA;
- NIST;
- COBIT.

2.3 List reputable sources of architectural patterns and guidance.

- NCSC;
- NIST;
- Vendors.

3. Developing a 'Security Case' (42.5%, K2)

In this key topic, the apprentice will understand how to develop a ‘security case’, recognising that threats evolve and threats also respond to a security design. Outcomes should include an ability to:

3.1 Describe the purpose of a security case.

3.2 List the key characteristics of a security case.

- business context;
- security objectives;
- threats and vulnerabilities;
- mitigation options;
- technical controls;
- organisational controls;
- cost benefit considerations;
- legal and regulatory environment;
- implementation activities.

3.3 Describe the resources available to aid with the development of a security case and how they can be used.

- Common Criteria;
- FIPS 140;
- NCSC CAPS.

3.4 Describe how threats can be modelled using the STRIDE example.

- Spoofing;
- Tampering;
- Repudiation;
- Information disclosure;
- Denial of service;
- Elevation of privilege.

3.5 Describe how threats change in response to security architecture and how threat modelling may need to change as a result of the outcome.

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.	11
2. Security Architectures	12
3. Developing a 'Security Case'	17
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

Recommended Reading List

Title: Security Architect
Author: Jon Collins
Publisher: BCS, The Chartered Institute for IT
Publication Date: 1st Sep 2014
ISBN-13: 9781780172200

Title: Business Cases That Get Results
Author: Carrie Marshall
Publisher: BCS, The Chartered Institute for IT
Publication Date: 31st Jan 2019
ISBN-13: 9781780174556