BCS Level 4 Award in Risk Assessment Syllabus QAN 603/0866/7

Version 1.1
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 Award in Risk Assessment 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

Introduction

This award is the sixth of seven knowledge modules that are applicable to the Level 4 Cyber Security Technologist Apprenticeship and is part of the Risk Analyst learning pathway. This is a general introduction to Cyber Security Risk and it examines the generic, high-level approach to risk management. It details the concepts of risk management and how one or more risk management approaches can be applied in an organisation.

Objectives

Apprentices should be able to demonstrate an understanding of information security and / or cyber risk management. Key areas are:

1. Principles of risk management.
2. Generic and published frameworks for risk management.
3. Threats, vulnerabilities and attacks.
4. Risk treatment.

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 Cyber Security risk and methodologies.

Course Format and Duration

Apprentices can study for this award by attending a training course provided by a BCS accredited Training Provider. The estimated total qualification time for this award is 58 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 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 Training Providers

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. Risk Assessment: Theory (25%, K3)

In this key topic, the apprentice will describe and explain how to manage information security, cyber risks and threats efficiently and effectively within an organisation. Outcomes should include an ability to:

1.1 Understand the principles and terminology of risk; for example, but not limited to:
- Probability
- Likelihood
- Threat
- Vulnerability
- Impact
- Threat actor
- Risk owner

1.2 Understand and describe the five key steps in risk management:
- Identify assets
- Identify threats and vulnerabilities
- Assess the impact of threats and vulnerabilities on an organisation
- Identify ways to manage those threats and vulnerabilities
- Monitor and report on risk management action

1.3 Discuss qualitative and quantitative approaches to risk assessment; including, but not limited to:
- Quantitative approaches (such as loss expectancy approaches (SLE/ARO))
- Quantitative scalar approaches (such as High/Medium/Low)

1.4 Illustrate how the results of an assessment can be presented; for example, but not limited to:
- Financial impact
- Dashboards
- Heat maps
- RAG.

2. Risk Assessment: Threat and Vulnerabilities (25%, K3)

In this key topic, the apprentice will demonstrate an understanding of the differences of threats and vulnerabilities. Outcomes should include an ability to:

2.1 Define and state the differences between:
- Threat
- Vulnerability
- Exploit
- Attack

2.2 Describe and explain the following:
- Categories of threats
- The concept of a threat lifecycle
- The use of threat intelligence in an organisation
- The uses of attribution

2.3 Discuss vulnerabilities, especially those relating to people and staff. Apprentices will understand how they can be exploited to attack an organisation; including, but not limited to:
- Phishing
- Social engineering
- Blended attacks

2.4 Describe common methods for finding vulnerabilities; for example, but not limited to:
- Penetration testing
- Phishing simulators
- Social engineering attacks

3. Risk Assessment: Standards (25%, K3)

In this key topic, the apprentice will explore factors relating to the standards surrounding cyber risk assessment. Outcomes should include an ability to:

3.1 Explain that risk assessment can be carried out using several methodologies or frameworks, but that it is better to select one methodology or framework for consistent and comparable results.

3.2 List the common risk assessment methodologies or frameworks; including, but not limited to:
- ISO/IEC 27005
- NIST Risk Management Framework
- OCTAVE
- FAIR

3.3 Compare common risk methodologies/frameworks; highlighting similarities and differences.

3.4 Demonstrate how to select and then apply a risk methodology/framework in an organisation.

4. Risk Assessment: Practice (25%, K3)

In this key topic, the apprentice will describe and explain how to apply a risk assessment methodology in an organisation. Outcomes should include an ability to:

4.1 Demonstrate how a risk assessment methodology/framework can be applied in an organisation to one or more of the following:
- Systems
- Applications
- Networks and information

4.2 Illustrate how vulnerabilities can be identified using a range of tools and techniques; including, but not limited to: research and technical.

4.3 Compare approaches to treating risk; for example, but not limited to:

- Accept
- Transfer
- Avoid
- Mitigate

Apprentices should also supply examples of how these approaches to treating risk can be achieved in practice; including, but not limited to: applying technical security controls to protect a system.

4.4 Discuss the role of risk owner and compare that role with other stakeholders.

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. Risk Assessment: Theory. (25%, K3)	10
2. Risk Assessment: Threat and Vulnerabilities. (25%, K3)	10
3. Risk Assessment: Standards. (25%, K3)	10
4. Risk Assessment: Practice. (25%, K3)	10
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)	58 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