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

Version 3.0
March 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 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
Version 2.0 September 2019	Update to branding, minor amends to wording and formatting. LO 1.4 wording amended for clarity.
Version 3.0 March 2020	Full syllabus review.

Introduction

This award is the second of the three knowledge modules that are applicable to the Risk Analyst pathway for the Level 4 Cyber Security Technologist Apprenticeship. This module 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:

- Describe relevant risk assessment methodologies commonly used in the context of information security and know how to apply in practice.
- Identify the vulnerabilities in organisation's 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 organisation's '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.

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

This award is relevant to anyone enrolled in the Level 4 Cyber Security Technologist Apprenticeship programme, requiring an understanding of cyber security risk assessment.

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 119 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 Methodologies (27.5%, K2)

In this key topic, the apprentice will describe relevant risk assessment methodologies commonly used in the context of information security and know how to apply them in practice. Outcomes should include an ability to:

1.1 Describe how vulnerabilities and threats combined with likelihood and impact create risk and describe the potential business consequences of the impact in terms of:
- Confidentiality;
- integrity;
- availability;
- productivity;
- financial;
- legal and regulatory;
- health and safety;
- reputation.

1.2 Describe commonly used risk assessment methodologies and their features:
- ISF Information Risk Assessment Methodology 2 (IRAM2);
- ISACA Risk IT;
- NIST SP 800-30;
- Octave;
- Factor Analysis of Information Risk (FAIR).

1.3 Explain how risk assessment methodologies are used in different types of organisations and situations:
- component-driven;
- system-driven;
- SMEs;
- Enterprises;
- public sector;
- military;
- CNI.

2 Threats and Vulnerabilities (47.5%, K2)

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

2.1 Describe the main sources of vulnerabilities and how to identify their relevance in various circumstances:
- OWASP Top 10;
- hardware design and implementation;
- software design and development;
- inadequate testing;
- poor configuration and integration;
- poor patch management;
- inadequate network defences;
- lack of encryption or access controls;
- lack of training and awareness;
- poor or missing documentation;
- inherent environmental factors;
- lack of monitoring - lack or auditing;
- poor policy and process;
- weak security culture;
- organisational change e.g. M&A.

2.2 Explain how organisational (management, training, policy and procedure) and technical (physical and logical) security can be linked to create new vulnerabilities or change their severity, including how people can be the weak link or greatest asset:

2.3 Describe what 'cyber culture' in an organisation is and how it can be improved or diminished e.g.:
- management commitment
- Accountability;
- employee awareness campaigns;
- employee training;
- rewards and punishments;
- employment contracts;
- policies and procedures;
- what incidents occur and how they are managed;
- whistleblowing.

2.4 Describe the main sources of threats and threat actors and how to identify their relevance in various circumstances with reference to:

- threat categories and models:
  - environmental event;
  - hardware failure;
  - software failure;
  - capacity problems;
  - information theft;
  - information disclosure;
  - malware;
  - phishing;
  - DOS and DDOS;
  - ransomware and crypto mining;
  - Microsoft STRIDE;
  - CVSS.
- threat actors (opportunity, motive, capability):
  - insiders;
  - individuals;
  - political groups;
  - activists;
  - organised crime;
  - state sponsored.

2.5 Describe threat intelligence sources and explain the intelligence lifecycle.

- Sources;
  - government e.g. NCSC;
  - commercial feeds;
  - vulnerability databases;
  - OSINT;
  - industry forums;
  - in-house expertise and internal systems;
  - dark web, social media and forums;
- lifecycle;
  - direction;
  - collection;
  - processing;
  - analysis;
  - dissemination;
  - feedback.

3 Risk Management in Practice (25%, K2)

In this key topic, the apprentice will describe different approaches to risk treatment and management. Outcomes should include an ability to:

3.1 Describe the steps in risk treatment and explain when the various treatment options might be appropriate in relation to risk appetite with reference to.

- ISO27005
  - Reduce;
  - Retain;
  - Avoid;
  - Transfer;
- NIST SP 800-30
  - Assumption;
  - Avoidance;
  - Limitation;
  - Planning;
  - Research and Acknowledgement;
  - Transference.

3.2 Explain the role of risk owner and how their view of risk may differ from that of other stakeholders who may have other financial or operational priorities:

3.3 Describe the features, benefits and drawbacks of qualitative and quantitative risk measurement methods and when each might be used.

- qualitative using:
  - 3x3 or 5x5 grid with likelihood and impact leading to low medium and high risks
- quantitative using:
  - Exposure Factor (EF);
  - Single Loss Expectancy (SLE);
  - Annualised Rate of Occurrence (ARO);
  - Annualised Loss Expectancy (ALE).

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 Methodologies	11
2. Threats and Vulnerabilities	19
3. Risk Management in Practice	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)	119 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

Title: Information Risk Management: A practitioner's guide
Author: David Sutton
Publisher: BCS, The Chartered Institute for IT
Publication Date: 26 Nov 2014
ISBN-13: 9781780172651

Title: Cyber Security: A practitioner's guide
Author: David Sutton
Publisher: BCS, The Chartered Institute for IT
Publication Date: 10 Jul 2017
ISBN-13: 9781780173405