BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Standards Syllabus
QAN 603/0855/2

Version 5.1
January 2019

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 Governance, Organisation, Law, Regulation and Standards

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 Jan 2017	Changes required to international standards text
Version 2.0 Mar 2017	Changes to K Levels and removal of topic area 8. Amendment to numbering in Key Topic 2 and change from Certification to Certificate in Learning Outcome 7.3
Version 3.0 Oct 2017	Syllabus re-developed
Version 3.1 Dec 2017	Topic area weightings and question weighting updated. Change from Investigatory Powers Act to Regulation of Investigatory Powers Act in Learning Outcome 5.1
Version 3.2 Feb 2018	Minor correction to Syllabus title spelling.
Version 4.0 April 2018	Addition of learning outcome 4.3.
Version 4.1 April 2018	Learning outcomes 4.3 and 4.4 swapped as error made in version 4.0
Version 5.0	Amendment of learning outcome 7.1 to provide clarity. Reasonable adjustments link amended.
Version 5.1 January 2019	Amendment to learning outcome 5.2. 17025 changed to 17021.

Introduction

This certificate is the last of seven knowledge modules that are applicable to the Level 4 Cyber Security Technologist Apprenticeship. This is a general introduction to the legal and regulatory aspects of cyber security.

The certificate is relevant to anyone requiring an understanding of Governance, Organisation, Law, Regulation and Standards including Security Operations Managers, Security Analysts, Risk Analysts, Security Architects and Information Governance Managers.

Objectives

Apprentices should be able to demonstrate knowledge and understanding of known security threats and how they can be mitigated. Key areas are:

- Understands, at a deeper level than from Knowledge Module 1, the legal, standards, regulations and ethical standards relevant to cyber security: governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver identified security outcomes.
- Has an awareness of the legal framework, key concepts applying to ISO27001 (a specification for information security management), and awareness of legal and regulatory obligations for breach notification.

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 on the Level 4 Cyber Security Technologist Apprenticeship programme.

Course Format and Duration

Candidates 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 127 hours.

Eligibility for the Examination

Individual employers will set the selection criteria, but this is likely to include 5 GCSEs (especially English, mathematics and a science or technology subject); other relevant qualifications and experience; or an aptitude test with a focus on IT skills.
Level 2 English and Maths will need to be achieved, if not already, prior to taking the endpoint assessment.

Format and Duration of the Examination

The format for the examination is a 1-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 Access to Assessment policy for detailed information on how and when to apply.

Additional time for Apprentices whose language is not the language of the examination

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: first, 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; second, to guide the proportion of questions in the exam. Training providers 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. Governance – Need, Purpose and Implementation (25%, K2)

In this topic, the apprentice will be able to explain the need for appropriate governance, organisational structure, roles, policies, standards and guidelines for cyber and information security, and how they work together to deliver identified security outcomes. The successful apprentice should be able to:

1.1 Explain why governance, organisational structure, roles, policies, standards and guidelines are needed to manage information security by describing how an organisation can:

- Align information security with business strategy;
- Manage risks appropriately;
- Manage resources efficiently and effectively;
- Measure performance;
- Deliver value by optimising information security investments.

1.2 Describe a model information security management structure by explaining the roles and purposes of:

- Governance bodies:
  - the Main Board;
  - the Risk Management Committee;
  - the Information Security Management Board.
- Governance roles:
  - the Main Board;
  - executives;
  - audit;
  - information security.
- Management planning:
  - strategic direction;
  - objectives setting;
  - risk management;
  - responsible resource use.
- Accountability and responsibility.
- Appropriate business fit for security - ensuring security aligns with organisational objectives, risk environment and culture.

1.3 Understand and explain how the various elements within an information security management structure operate together to deliver the required security outcomes using the concepts of:

- Ownership;
  - risk;
  - asset;
  - process ownership.
- Delegation.
- Custodianship.

1.4 Describe how organisations can use the elements below to integrate information security into the overall corporate governance and application development process, ensuring effective delivery of security outcomes:

- The change management process.
- Embedding security into project management practices.

1.5 Recognise how legislation and regulation can be implemented in a manner that meets specific, local information security risks:

- Ensuring appropriate connections between legislation, regulation, policy, risk management and project management.

2. Access Control support for Governance (5%, K2)

In this topic area, the apprentice will be able to explain how an organisation's security policies, standards and governance are supported by provisioning and access rights (e.g. how identity and access management are implemented and maintained for a database, application or physical access control system). The successful apprentice should be able to:

2.1 Describe how effective management of identity provisioning and access rights support an organisation's security policies, standards and governance via:

- Password management;
- Role based access control (RBAC);
- The principle of 'least privilege';
- Privileged access management;
- Principles of identity access management for access to databases, applications and physical environments;
- Physical access control tools:
  - swipe cards.
  - PINs.
  - biometrics.

3. Policies and procedures in different organisational environments (17.5%, K2)

In this topic area, the apprentice will be able to describe how cyber security policies and procedures are used in different organisational environments and affect individuals and organisations. The successful apprentice should be able to:

3.1 Describe an organisational environment and the factors and forces that shape it through:

- General environment, task environment and internal environment.
- The components of an internal environment:
  - management;
  - employees;
  - shareholders;
  - representative bodies.
- The major forces in the external environment:
  - political;
  - economic;
  - technological;
  - socio-economic;
  - legal and regulatory.

3.2 Explain how an organisation's type can affect the way it manages information security and how internal and external forces impact on security management in the following types of organisations:

- Central government;
- Financial services;
- Healthcare;
- Aerospace and defence;
- Utilities;
- Social services.

3.3 Describe the impact of the following regulations on the associated organisations:

- HIPAA (healthcare);
- Sarbanes-Oxley (Listed companies with US presence);
- Basel III (international finance);
- PCI-DSS (all businesses that use credit cards);
- IASME (Small to Medium sized enterprises);
- NIST (US government and international defence).

3.4 Describe the impact of the General Data Protection Regulation (GDPR) on the following sectors, and identify what actions should be taken to meet the Regulation:

- Government (both central and local) - including Social and Child Protection Services;
- Financial Services;
- Healthcare;
- Law enforcement.

4. Security Expert Roles and information providers (20%, K2)

In this topic area, the apprentice will be able to understand the roles of experts in the cyber security industry, how they are recognised, and the work they do. The successful apprentice should be able to:

4.1 List and understand the key characteristics of the main specialist roles associated with information security, which are:

- Internal:
  - Chief information security officer (CISO);
  - Security operations centre (SOC) analyst;
  - Penetration tester / ethical hacker;
  - Governance, risk and compliance (GRC) manager;
  - Security architect;
  - Operational security manager.
- External:
  - Vulnerability assessors;
  - Penetration testers;
  - Auditors: ISO 27001 auditors.
  - HMG accreditors.

4.2 Describe the purpose of the main professional qualifications for an information security specialist:

- Certified Information Systems Security Professional (CISSP);
- Certified Information Security Manager (CISM);
- CESG Certified Practitioner (CCP);
- BCS ISEB Certificate in Information Security Management Principles (CISMP);
- Certified Information Systems Auditor (CISA);
- Certification and Accreditation Professional (CAP);
- Global Information Assurance Certification (GIAC);
- Lead ISO 27001 Auditor;
- Internal ISO 27001 Auditor;
- CHECK Team Leader.

4.3 Explain the main information security roles that tend to be undertaken by, often external specialists:

- Vulnerability assessors;
- Penetration testers;
- Auditors;
  - ISO 27001 auditors;
- HMG accreditors.

4.4 Summarise the typical responsibilities of an information security team:

- Security operations management:
  - Security Operations Centres (SOCs);
  - fraud investigation;
  - data flow control.
- Governance, risk and compliance (GRC);
  - regulation management;
  - change approval;
  - GRC document management;
  - compliance.
- Internal and external audit:
  - audit event management;
  - logistical support.

4.5 Understand the role and purpose of security intelligence information and how to obtain and use these.

- CERT (Computer Emergency Response Team);
- UK National Cyber Security Centre;
- Publicly available government sources (Open Source Intelligence provider);
- Professional and academic publications;
- Commercial information;
- 'Gray literature' (working papers, unpublished resources).

5. Legal Framework (10%, K2)

In this topic area, the apprentice will demonstrate a clear awareness of the legal framework surrounding intelligence gathering and the relationship to data protection, human rights and privacy. The successful apprentice should be able to:

5.1 Explain how the legislation listed below interacts to support security, privacy, data protection, monitoring and investigations:

- Data Protection Act / GDPR;
- Human Rights Act;
- Regulation of Investigatory Powers Act.

5.2 Recognise the key security standards that impact information security:

- The ISO 27000 series of standards;
- The US National Institute of Standards and Technology (NIST) standards publications;
- The Information Security Forum (ISF) Standard of Good Practice (SOGP);
- The National Cyber Security Centre (NCSC) standards:
  - CESG Assisted Products Service;
  - Commercial Products Assurance.
- The Payment Card Industry Data Security Standard (PCI-DSS);
- ISO/IECs 15408, 17021 and 20000.

6. Applying ISO 27001:2013 (12.5%, K2)

In this topic area, the apprentice will be able to explain the key concepts and benefits of applying ISO27001 to implement an information security management system. The successful apprentice should be able to:

6.1 Explain what an Information Security Management System (ISMS) is.

6.2 Explain the key concepts of ISO27001.

6.3 Explain how an organisation obtains certification to ISO/IEC 27001.

6.4 State the benefits of certification to ISO/IEC 27001.

7. Security Breach Notification (10%, K2)

In this topic area, the apprentice will demonstrate a clear awareness of legal and regulatory obligations for breach notification. The successful apprentice should be able to:

7.1 Explain that the General Data Protection Regulations (GDPR), Article 33, makes data breach reporting mandatory to the Information Commissioners Office (ICO). Apprentices must be able to explain the impact of a breach in security and the unauthorised release of personal data with relation to the following legislation:

- The Privacy and Electronic Communications Regulations (PECR);
- The Human Rights Act (HRA);
- Data Protection Act (DPA).

7.2 List, in relation to the UK Data Protection Act and the GDPR:

- The specific time periods permitted within which information security breaches should be reported.
- The authorities that require notification.
- The means by which notification can be undertaken.

Levels of Knowledge / SFIA Levels

This syllabus 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 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. Governance - need, purpose and implementation	10
2. Access Control support for Governance	2
3. Policies and procedures in different organisational environments	7
4. Security Expert Roles and information providers	8
5. Legal Framework	4
6. Applying ISO 27001:2013	5
7. Security Breach Notification	4
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	Training from a BCS accredited training provider 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)	127 hours, 85 GLH recommended.
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