Making IT good for society

BCS Level 4 Certificate in Information and Cyber Security Foundations Syllabus 603/3214/1

Version 1.0
April 2018

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.

Making IT good for society

BCS Level 4 Certificate in Information and Cyber Security Foundations 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
V1.0	Document created.

Introduction

This certificate is the third module of five knowledge modules that are applicable to the level 4 Cyber Intrusion Analyst apprenticeship. This is a general introduction to information and cyber security foundations, for which apprentices are required to demonstrate their knowledge and understanding.

Objectives

Apprentices should be able to demonstrate an understanding of information and cyber security foundations. Key areas are:

1. Explaining the importance of cyber security and basic concepts including harm, identity, confidentiality, integrity, availability, threat, risk and hazard, trust and assurance and the 'insider threat'.
2. Explaining how the concepts relate to each other and the significance of risk to a business.
3. Understanding and proposing appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment.
4. Understanding and proposing how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment.

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 certificate is relevant to anyone enrolled on the Level 4 Cyber Intrusion Analyst Apprenticeship programme.

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 233 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.

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 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 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: 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 Cyber Security Fundamentals (5%, K2)

In this topic area, the apprentice will understand basic cyber security concepts and their importance to organisations. The successful apprentice should be able to:

1.1 Describe why cyber security is important to organisations.
- large corporations;
- SMEs.

1.2 Explain how the basic concepts of cyber security can relate to each other.
- identity;
- availability;
- integrity;
- confidentiality;
- assurance;
- threat;
  - external;
  - internal;
- risk;
- hazard;
- harm.

2 Risk Assessment and Management (25%, K2)

In this topic area, the apprentice will understand risk assessment, management and investigation. The successful apprentice should be able to:

2.1 Explain how risk assessment and management can benefit an organisation.

2.2 Understand the common terminology, controls and approaches used in risk assessment and management.
- vulnerabilities and exploitabilities;
- controls.

2.3 Understand the types of risks, threats and vulnerabilities, and how they can impact an organisation.

- spoofing of user identity;
- tampering;
- repudiation;
- information disclosure (privacy breach or data leak);
- Denial of Service (DoS);
- elevation of privilege.

2.4 Describe the main stages and principles of risk assessment, control and management.

- components of risk;
  - threat;
  - likelihood;
  - impact;
- five step composite risk management process;
  - identify hazards;
  - assess hazards to determine risks;
  - develop control measures that eliminate the hazard or reduce its risk;
  - implement controls that eliminate the hazards or reduce their risks;
  - evaluate the effectiveness of controls and adjust / update as necessary;
- threat modelling;
  - STRIDE (Microsoft);
    - Spoofing of user identity;
    - Tampering;
    - Repudiation;
    - Information disclosure (privacy breach or data leak);
    - Denial of Service (DoS);
    - Elevation of privilege;
  - P.A.S.T.A. (Process for Attack Simulation and Threat Analysis);
  - Trike (a risk-based approach with distinct implementation, threat, and risk models);
  - VAST (Visual, Agile, and Simple Threat modelling);
- impact levels.

2.5 Identify sources of information about threats and vulnerabilities from relevant industry sources.

- critical vendors;
- governmental and public sources;
- private sources.

2.6 Explain how poor security management can adversely impact an organisation.

2.7 Describe the common causes of security incidents.
- weak and stolen credentials;
- back doors, application vulnerabilities;
- malware;
- social engineering;
- inappropriate permissions granted;
- insider threats;
- physical attacks;
- improper configuration.

2.8 Identify security controls that relate to:
- people;
- process;
- technology.

2.9 Describe the different types of tests that can be used to prepare an organisation.
- security auditing;
- vulnerability testing;
- penetration testing.

2.10 Describe security processes and procedures used within own organisation to maintain operational security.

3 Information Governance (27.5%, K2)

In this topic area, the apprentice will describe and explain all aspects of information governance including policy, legal and regulatory environment, information assurance, information security awareness and audit. The successful apprentice should be able to:

3.1 Explain the term information governance and the potential impacts of poor information governance.

3.2 Recognise the need for information security policy to achieve information security.

3.3 Describe what an information security management system (ISMS) is and the potential benefits.

3.4 Describe and explain the following aspects of providing information assurance:
- methodologies;
  - ISO/IEC 27001;
  - ISO/IEC 27005;
- processes;
  - staff awareness raising / training;
  - backups;
  - configuration hardening;
- standards;
  - ISO/IEC 27002;
  - COBIT.

3.5 Describe and explain information assurance methodologies.
- ISO/IEC 27000 series;
  - ISO/IEC 27001;
  - ISO/IEC 27002;
- Risk IT;
- COBIT.

3.6 Identify industry standards bodies and services and provide examples of the services that they provide.
- BSI (British Standards Institute);
  - product certification;
  - personal training and certification;
- IAAC (Information Assurance Advisory Council);
  - development of policy recommendations to government and corporate leaders;
  - free workshops.

3.7 Explain how security awareness and training provides benefits to the maintenance of information security.

3.8 Describe a variety of methods for improving security awareness.
- mandatory cyber awareness training;
- management leading by example;
- interactive materials;
  - gamification;
  - video;
- multi vector approach;
  - posters;
  - blogs;
  - e-mail tips;
  - newsletters.

3.9 Identify examples of information security risks caused by poor security awareness.
- principle of least privilege (POLP) not implemented;
- poor password discipline;
- account sharing;
- accessing of unsafe internet locations;
- installation of non-approved software.

3.10 Explain how audits and reviews contribute to effective security management.

3.11 Identify common sources of information, standards, legislation and accreditation boards that are used to drive and control audit and review processes and practitioners.
- BSI (British Standards Institute);
- IAAC (Information Assurance Advisory Council);
- ISACA (Information Systems Audit and Control Association);
- ISSA (Information Systems Security Association (international));
- BCS (British Computer Society).

3.12 Outline the governance controls used within your own organisation.

3.13 Describe local processes for consultation, review and approval.

3.14 Describe audit and review controls used within own organisation.

4 Security Architecture (7.5%, K2)

In this topic area, the apprentice will demonstrate an awareness of security architecture. The successful apprentice should be able to:

4.1 Describe the concept of information security architecture and how it can be used to reduce information risk.

4.2 Explain how information security architecture interacts with other enterprise architectures.

4.3 Describe how security architecture relates to business needs.
- Does the nature of the business lead to specific security vulnerabilities?
  - e-commerce;
  - child related (schools or colleges);
  - confidential data related (medical, defence or judicial);
  - social media;
- Does the security architecture provide obstacles to the main business activities?
- Will the current security architecture support future developments of the business?

4.4 Understands design patterns or architecture relevant to own work.

5 Business Continuity Management (10%, K2)

In this topic area, the apprentice will describe and explain business continuity management approaches, benefits and its relationship with incident management. The successful apprentice should be able to:

5.1 Explain the benefits of business continuity management (BCM) and the consequences of poor BCM.

5.2 Explain the relationship of BCM with incident management.

5.3 Describe the steps within the BCM lifecycle and the approaches that can be used to provide business continuity.

- ISO 22301;
  - impact analysis - BIA and TRA;
  - solution design;
  - implementation;
  - testing and organisational acceptance;
  - maintenance.

6 Responding to Attacks (15%, K3)

In this topic area, the apprentice will understand how to recognise and respond to an attack. The successful apprentice should be able to:

6.1 Describe the possible indicators (signatures) of compromise.

- virus signatures;
- MD5 hashes or IP addresses of known malware;
- known domains or URLs of botnets;
- unusual outbound network traffic;
- unusual privilege account use;
- DNS request anomalies;
- web traffic with unhuman behaviour;
- signs of DDoS activity.

6.2 Describe the difference between targeted and general and systemic attacks.

6.3 Describe the response options that are available and the main features to implement each.

- containment;
- eradication;
- exploitation;
- legal.

6.4 Describe how to scope a response given the objectives for the system under threat.

6.5 Describe the process and the benefits of timeline analysis.

- data sources;
  - audits;
  - event logs;
  - file change timestamps and metadata;
    - MTF (Windows);
    - Inode (Linux);
  - tools;
    - Log2timeline;
    - packet sniffers;
    - Plaso;
    - TimeFlow;
- benefits;
  - timeline presents complex data in a more human friendly accessible format.

6.6 Prepare action plans based on previous intrusions to reduce the risk of future attacks.

7 Emerging Threats (10%, K3)

In this topic area, the apprentice will understand the current cyber security threat landscape and recognise emergent attacks. The successful apprentice should be able to:

7.1 Identify the current cyber security threat landscape.

- known attack techniques;
  - cross-site scripting (XSS);
  - Denial of Service attacks;
  - malware attacks;
  - man-in-the-middle (MITM) attacks;
  - phishing attacks;
  - SQL injection attacks (SQLi);
- hazards;
  - IoT (increased vulnerability surface);
  - ransomware;
- vulnerabilities;
  - buffer overflow;
  - lack of encryption;
  - lack of patch management;
  - poor staff security awareness;
  - weak passwords.

7.2 Recognise emergent attack techniques, hazards or vulnerabilities.

- be aware that it is a constantly changing threat environment;
  - monitor information sources;
    - news feeds and alerts;
    - academic research;
    - hacker forums;
  - evaluate potential emergent attacks against known techniques.

7.3 Describe what assets are affected by an emerging threat and the impact to an organisation.

- data;
- hardware;
- software;
- configuration settings;
- staff;
- buildings and infrastructure.

7.4 Describe how a signature or correlation rule is developed in response to the following attack techniques:

- intrusion events;
- malware events;
- abnormal user activity;
- traffic profile changes.

7.5 Demonstrate how to write a signature or correlation rule.

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. Cyber Security Fundamentals	2
2. Risk Assessment and Management	10
3. Information Governance	11
4. Security Architecture	3
5. Business Continuity Management	4
6. Responding to attacks	6
7. Emerging threats	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)	233 Hours, 97.5 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