BCS Level 3 IT Solutions Technician Digital IT Apprenticeship End-point Assessment Knowledge Unit

Security and Legislation Syllabus

Version 1.2
May 2020

BCS Level 3 IT Solutions Technician Digital IT Apprenticeship End-point Assessment Knowledge Unit – Security and Legislation

Contents

Introduction 4

Objectives 4

Eligibility for the Examination....4

Format and Duration 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 Examination5

Syllabus 6

Levels of Knowledge / SFIA Levels 10

Question Weighting 10

Format of Examination 10

Recommended Reading List 11

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 February 2020	Document created.
V1.1 February 2020	Update to learning outcome 2.1 to align better with the Computer Misuse Act.
V1.2 May 2020	Removal of “Training Criteria” and “Classroom size” sections as not applicable.

Introduction

This is the last unit of the four knowledge units required for the Level 3 IT Solutions Technician Apprenticeship and forms part of the end-point assessment. It covers the range of concepts, approaches and techniques that are applicable to security and legislation relevant to IT solutions, for which apprentices are required to demonstrate their knowledge and understanding.

Objectives

Apprentices should be able to demonstrate knowledge and understanding of IT solution security and legislation. Key areas are:

1. Understands the key features of, and where to find, organisational requirements in relation to policies, standards, legislation, professional ethics, privacy and confidentiality.
2. Understands the main legislation, policies and standards that apply to IT solutions.
3. Understands how their work contributes to business performance, continuity and resilience.
4. Understands why cyber security is essential as part of the delivery of any solution.
5. Understands the importance of working securely and the main classifications of types of threats and common mitigation practices.
6. Understands the meaning of risk in the context of security and can explain the relationship between levels of risk, impact, and designed level of protection in IT Solutions.

Evidence of lessons learnt in these key areas should be collected and reflected upon when the apprentice is compiling the portfolio as the apprentice could identify how the task might be done better / differently with knowledge subsequently gained.

Target Audience

The syllabus is relevant to anyone enrolled on the Level 3 IT Solutions Technician apprenticeship programme.

Eligibility for the Examination

Apprentices must be enrolled on the level 3 IT Solutions Technician Digital IT apprenticeship and have entered end-point assessment gateway. Level 2 English and Maths will need to be achieved, if not already, prior to taking the end-point assessment.

Format and Duration of the Examination

The format for the examination is a 30-minute multiple-choice examination consisting of 20 questions. The examination is closed book (no materials can be taken into the examination room). The pass mark is 13/20 (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 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.

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 Organisational Requirements (10%, K1)

In this topic, the apprentice will understand the key features of, and where to find, organisational requirements in relation to policies, standards, legislation, professional ethics, privacy and confidentiality. The successful apprentice should be able to:

1.1 List the key features of:
- policies;
- standards;
- legislation;
- professional ethics;
- privacy;
- confidentiality.

1.2 Describe where in any organisation the policies, standards, legislation, professional ethics, privacy and confidentiality documentation could be found.
- employee handbook;
- company intranet;
- internal training courses.

2 Legislation, Policies and Standards (20%, K2)

In this topic area, the apprentice will understand the main legislation, policies and standards that apply to IT solutions. The successful apprentice should be able to:

2.1 Describe the main offences of Computer Misuse Act 1990.
- unauthorised access to computer material;
- unauthorised access with intent to commit or facilitate commission of further offences;
- unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer.

2.2 Explain the importance of the ISO/IEC 27000 series of standards.

2.3 Explain the 'Integrity and Confidentiality Principle' (the Security Principle) of the GDPR and describe the roles of 'Controller' and 'Processor' in relation to GDPR and how they apply to IT Solutions.

3 Business Performance, Continuity and Resilience (15%, K2)

In this topic area, the apprentice will understand how their work contributes to business performance, continuity and resilience. The successful apprentice should be able to:

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

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

- ISO 22301;
  - impact analysis – business impact analysis (BIA) and threat and risk assessment (TRA);
  - solution design;
  - implementation;
  - testing and organisational acceptance;
  - maintenance.

4 Cyber Security for IT Solutions (20%, K2)

In this topic area, the apprentice will understand why cyber security is essential as part of the delivery of any solution. The successful apprentice should be able to:

4.1 Describe the key elements of cyber security.

- identity;
- availability;
- integrity;
- confidentiality;
- assurance;
- threat;
  - external;
  - internal;
- risk;
- hazard;
- harm.

4.2 Identify security controls that relate to the following when delivering any IT solution:

- people;
- process;
- technology.

4.3 Describe the following methods for improving cyber security awareness as part of any IT Solution delivery:

- mandatory cyber awareness training;
- management leading by example;
- interactive materials;
- gamification;
- video;
- multi vector approach;
- posters;
- blogs;
- e-mail tips;
- newsletters.

5 Working Securely (20%, K2)

In this topic area, the apprentice will understand the importance of working securely and the main classifications of types of threats and common mitigation practices. The successful apprentice should be able to:

5.1 Explain the importance of working securely.

5.2 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.

5.3 Describe the following information security industry risk mitigation strategies:

- perimeter controls;
- traffic filtering;
- least privilege;
- authentication and authorisation;
- anti-malware;
- application whitelisting;
- proactive monitoring;
- secure configuration;
- intrusion detection and prevention;
- file integrity monitoring;
- data loss prevention;
- patching and updating;
- change control;
- encrypted connections.

6 Risk (15%, K2)

In this topic area, the apprentice will understand the meaning of risk in the context of security and can explain the relationship between levels of risk, impact, and designed level of protection in IT Solutions. The successful apprentice should be able to:

6.1 Describe the key features of an IT risk management strategy.

- identify;
- analyse;
- evaluate;
- monitor.

6.2 Describe and explain:

- what security risk is;
- how risks are quantified by likelihood and impact.

6.3 Describe the following levels of protection when delivering any IT solution.

- securing the network;
- securing devices;
- securing applications;
- O/S updates;
- anti-virus software;
- anti-malware.

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. Organisational Requirements	2
2. Legislation, Policies and Standards	4
3. Business Performance, Continuity and Resilience	3
4. Cyber Security for IT Solutions	4
5. Working Securely	4
6. Risk	3
Total	**20 Questions**

Format of Examination

Type	20 Question Multiple Choice.
Duration	30 minutes. An additional 25% 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	13/20 (65%).
Calculators	Calculators cannot be used during this examination.
Delivery	Online.

Recommended Reading List

Title: Information Security Management Principles
Author: David Alexander, Amanda Finch, David Sutton, Andy Taylor
Publisher: BCS, The Chartered Institute for IT
Publication Date: January 2020
ISBN-13: 9781780175188

Title: A Practical Guide to IT Law
Author: Victoria Hordern, Sara Ellacott, Michaela McDonald, Nikki Cordell, Andy Lucas, Andrew Katz, Stewart James, Stuart Smith
Publisher: BCS, The Chartered Institute for IT
Publication Date: August 2020
ISBN-13: 9781780174884