BCS Level 4 Applications Support Lead Apprenticeship

End-Point Assessment Knowledge Test

February 2022 v1.2

This is a United Kingdom government regulated qualification which is administered and approved by one or more of the following: Ofqual, Qualifications Wales, CCEA Regulation or SQA.

bcs
The Chartered Institute for IT

Document 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 December 2021	Syllabus created.
Version 1.1 January 2022	Syllabus review by SME. Corrections made.
Version 1.2 February 2022	Further changes made to the wording and content of the syllabus following review by SME.

bcs
The Chartered Institute for IT

CONTENTS

Introduction

An Applications Support Lead provides tactical advice, training and support on core technology applications (both hardware and software) to internal colleagues, external clients and customers to enhance and enable the delivery of application-based products and services.

An employee in this occupation will carry out a range of responsibilities including delivering the roll-out of upgrades to new and existing technologies, assisting in the planning of IT application and infrastructure change projects, and building, implementing and supporting the creation of remote working environments.

This Level 4 apprenticeship covers the key concepts, skills and tools required of anyone working in an Applications Support Lead role, to be able to confidently and successfully provide advice and guidance both to colleagues within an organisations and to external customers.

Qualification Suitability and Overview

There are no mandatory requirements for candidates to be able to undertake this certificate qualification, although candidates will need a good standard of written English and Maths. Centres must ensure that learners have the potential and opportunity to gain the qualification successfully.

This qualification is suitable for candidates who are looking to progress their career within an Application Support role. It can be taken as a standalone qualification, or in combination with other units and modules as part of a wider programme, such as an Apprenticeship.

This is an occupationally focused qualification which will:

- Test a learner's ability to recall and apply knowledge in a range of scenarios.
- Allow them to demonstrate a practical understanding of key concepts across the topic areas.
- Enable a learner to progress in their career.

Candidates can study for this certificate by attending a training course provided by a BCS accredited Training Provider or through self-study.

Learning Outcomes

Upon completion of the certificate candidates will be able to demonstrate:

- An understanding of the legal requirements relating to the use of data.
- An understanding of the legal requirements related to the provision of application support services.
- An understanding of the differences between structured and unstructured data.
- An understanding of how to use data ethically and the implications of data use for wider society.
- An understanding of security vulnerabilities and approaches to security testing including penetration testing.

K1 : awareness of the legal requirements relating to the use of data as set out in the GDPR 2016/679 and the Data Protection Act 2018.

K2 : awareness of the legal requirements related to the provision of application support services including the Malicious Communications Act 1988, the Copyright, Designs and Patents Act 1988, the Computer Misuse Act 1990 and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

K4 : the differences between structured and unstructured data.

K8 : how to use data ethically and the implications of data use for wider society.

K17 : security vulnerabilities and approaches to security testing including penetration testing.

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**

Syllabus

1. Legal requirements relating to the use of data (25%, K4)

Candidates will be able to:

1.1 Demonstrate an awareness around personal data rights in the EU and the UK:

Indicative content

a. Background to the rights to protect Personal Data in the EU and the UK
b. General Data Protection Regulation 2016/679
c. The purpose of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
d. UK Data Protection Act 2018, Part 2, Chapters 1 to 3, Parts 5 & 6
e. The role of the Information Commissioners Office (ICO) in data protection
f. The Freedom of Information Act 2000 (FOI)

Guidance

Apprentices should have a good overall knowledge of the different legislations that affect individuals and their personal data within the EU and UK.

They should understand the reasoning behind the legislation and also how this is split across different legislation.

Apprentices should be aware of who the Information Commissioners Office are, and what their responsibility is in relation to data.

1.2 Illustrate the content and coverage of GDPR in its entirety

Indicative content

a. Consent
b. Contract
c. Legal obligation
d. Vital interests
e. Public interest
f. Legitimate interests
g. Applicability
h. Consequences

Guidance

Apprentices should have a more specific understanding of the GDPR 2016/679 and how this applies to individuals both in the UK and Abroad. They should be aware of how this affects how an organisation both gathers and handles data.

Apprentices should be aware of the consequences to an organisation should they not meet the requirements.

1.3 Illustrate the content and coverage of the Data Protection Act 2018 in its entirety

Indicative content

a. Consent
b. Contract
c. Legal obligation
d. Vital interests
e. Public interest
f. Legitimate interests
g. Applicability
h. Consequences

Guidance

Apprentices should have a more specific understanding of the Data Protection Act 2018 and how this applies to individuals both in the UK and Abroad. They should be aware of how this affects how an organisation both gathers and handles data.

Apprentices should be aware of the consequences to an organisation should they not meet the requirements.

Syllabus

2.Legal requirements related to the provision of application support services (20%, K4)

Candidates will be able to:

2.1 Describe and interpret the Malicious Communications Act 1988

Indicative content

a. Main aims of the legislation
b. Applicability of legislation
c. Consequences of not meeting legal requirements

Guidance

Apprentices should be aware of what this legislation is, how it affects both individuals and organisations. They should be able to express business precautions that should be taken to protect an organisation against breaching this legislation and what could happen to an organisation should they breach it.

2.2 Describe and interpret the Copyright, Designs and Patents Act 1988

Indicative content

a. Main aims of the legislation
b. Applicability of legislation
c. Consequences of not meeting legal requirements

Guidance

Apprentices should be aware of what this legislation is, how it affects both individuals and organisations. They should be able to express business precautions that should be taken to protect an organisation against breaching this legislation and what could happen to an organisation should they breach it.

2.3 Describe and interpret the Computer Misuse Act 1990

Indicative content

a. Main aims of the legislation
b. Applicability of legislation
c. Consequences of not meeting legal requirements

Guidance

Apprentices should be aware of what this legislation is, how it affects both individuals and organisations. They should be able to express business precautions that should be taken to protect an organisation against breaching this legislation and what could happen to an organisation should they breach it.

2.4 Describe and interpret the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

Indicative content

a. Main aims of the legislation
b. Applicability of legislation
c. Consequences of not meeting legal requirements

Guidance

Apprentices should be aware of what this legislation is, how it affects both individuals and organisations. They should be able to express business precautions that should be taken to protect an organisation against breaching this legislation and what could happen to an organisation should they breach it.

Syllabus

3. Structured and unstructured data (10%, K2)

Candidates will be able to:

3.1 Describe the differences between structured and unstructured data.

Indicative content

a. Structured – ordered, organised data
b. Unstructured – no format, structure or apparent order

Guidance

Apprentices should be able to explain what both structured and unstructured data is, how this may be presented and be able to identify data given to them as either structured or unstructured.

3.2 Recognise common sources of structured data.

Indicative content

a. Data files organised sequentially or organised serially
b. Tables stored within a database management system
c. Extensible Markup Language.

Guidance

Apprentices should be able to identify a range of the most common sources of structured data within the IT industry, these may included various databases, software packages, web based sources – specific packages may be mentioned.

3.3 Explain that unstructured data can take various formats.

Indicative content

a. Word processor, spreadsheet and PowerPoint files
b. Audio
c. Video
d. Image
e. Sensor and log data
f. External data (such as social media feeds)
g. Paper-based documents

Guidance

Apprentices should be able to identify that these formats are all unstructured, the reasons why these are not structured. They should be able to select from a number of reasons why these cannot be structured formats.

3.4 Recognise how structured and unstructured data could complement each other to derive rich insight.

Indicative content

a. Enhance analysis of the other (Structured or Unstructured text data)
b. Combined into a common model
c. Big data analytics

Guidance

Apprentices should be able to explain the reasoning behind using a wide range of data, both structured and unstructured, within their role. How this data can both support the implementation of new technologies and support technologies in use within the organisation.

Syllabus

4.Ethical data and the implications of data use for wider society (20%, K2)

Candidates will be able to:

4.1 Understand and explain the range of different types of data and the implications for allowable use, data quality, privacy concerns and availability.

Indicative content

a. Open and public vs. proprietary data
b. Operational (data used in the day-to-day business operations) vs. administrative data (data used for the administration and management)
c. Research data

Guidance

Apprentices should be aware of the various different public interest concerns, and benefits, to the use of data by organisations. They should be aware of the different uses of data within a typical organisation and by the wider community.

4.2 Describe the data protection and privacy issues that can occur during data analysis activities.

Indicative content

a. Discuss the types, formats and activities that are protected:
   - Personally Identifiable Information
   - Protected Health Information

Guidance

Apprentices should be able to identify the different types of data that may be considered as sensitive or protected. They should be aware of why this data may be of more concern in relation to protection and privacy.

4.3 Recognise and explain the key principles of Data Protection legislation.

Indicative content

a. Lawfulness, fairness and transparency
b. Purpose limitation
c. Data minimisation
d. Accuracy
e. Storage limitation
f. Integrity and confidentiality (security)
g. Accountability

Guidance

Apprentices should be able to identify the 7 key principles of Data Protection and each of their purposes. They should be able to explain the reason behind each of these principles.

4.4 Explain the need to comply with Data Protection legislation.

Indicative content

a. Rights and obligations
b. Enforcement agencies
c. Regulatory and legal penalties

Guidance

Apprentices should be aware of the danger that organisations face should they breach Data Protection Legislation, they should be aware of the financial/legal penalties that they could face. They should also be aware of the impact that breaching can have on the public perception of the organisation.

Syllabus

5. Security vulnerabilities and approaches to security testing (25%, K2)

Candidates will be able to:

5.1 Describe common vulnerabilities in computer networks and systems.

Indicative content

a. Non-secure coding
b. Inadequate traffic filtering
c. Missing patches and updates
d. Inappropriate configuration
e. Insecure protocols
f. Lack of malware protection
g. Inadequate access controls (identification, authentication, authorisation, ACLs)
h. Inappropriate design and architecture
i. Lack of consideration of environmental factors
j. Inadequate physical security controls
k. Interoperability

Guidance

Apprentices should be able to describe what each security event listed might involve. For example, suspicious user behaviour might involve user logins that take place at an unusual time of day or the user trying to access information that they do not have permission to access. Apprentices will be able to explain the common detection and prevention methods available for each security event.

5.2 Describe what security objectives and security requirements are and what they should include.

Indicative content

a. Functional requirements
b. Non-functional requirements
c. Must have, Should have, Could have, Want to have (but won't have this time) (MoSCoW)
d. KPIs
e. Responsibility

Guidance

Apprentices should be able to describe what each security event listed might involve. For example, suspicious user behaviour might involve user logins that take place at an unusual time of day or the user trying to access information that they do not have permission to access. Apprentices will be able to explain the common detection and prevention methods available for each security event.

5.3 Describe information security events and explain how they can be detected and / or prevented.

Indicative content

Security event	Detective measure	Preventative measure
Brute force attack	• System logs • Multiple failed login attempts	• Failed attempt lockouts • Limiting simultaneous logins • Multi-factor authentication • Use of CAPTCHA technology
Malware activity • Ransomware • Worm • Trojans • Spyware	• System logs • Network logs • Intrusion Detection Systems • Security awareness training	• Anti-malware software • Firewalls • Intrusion Prevention Systems • Vulnerability/patch management
Suspicious user behaviour	• Honeypots • File Integrity Monitoring • Behavioural analytics • System logs • Network logs • CCTV	• Firewalls • Role-based access control • Principle of least privilege • Job rotation • Door entry system • Web proxy
Suspicious device behaviour	• Intrusion Detection Systems • System logs • Network logs	• Intrusion Prevention Systems • Firewalls
Unauthorized system changes	• System Integrity Monitoring • File Integrity Monitoring	• Role-based access control • Principle of least privilege

Guidance

Apprentices should be able to describe what each security event listed might involve. For example, suspicious user behaviour might involve user logins that take place at an unusual time of day or the user trying to access information that they do not have permission to access. Apprentices will be able to explain the common detection and prevention methods available for each security event.

5.4 Describe what security objectives and security requirements are and what they should include.

Indicative content

a. Pen test
b. Red team exercise
c. Bug/bounty hunter

Guidance

Apprentices should be aware of the role of security testing within an organisation, they should be aware of the purpose of testing and how this can support an organisation to improve their internal security processes.

Examination Format

This certificate is assessed through completion of an invigilated online exam which candidates will only be able to access at the date and time they are registered to attend.

Type	40 Multiple Choice Questions.
Duration	1 Hour.
Supervised	Yes.
Open Book	No (no materials can be taken into the examination room)
Passmark	24/40 (60%).
Delivery	Digital format only.

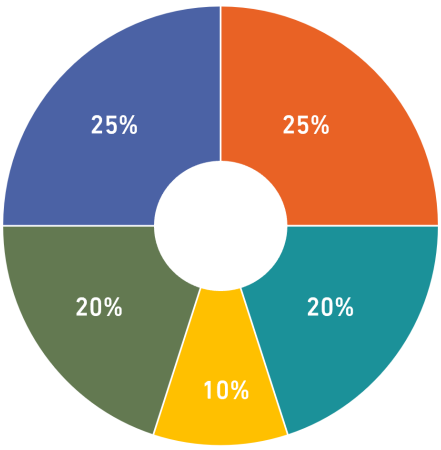
Adjustments and/or additional time can be requested in line with the BCS reasonable adjustments policy for candidates with a disability, or other special considerations including English as a second language.

Question Weighting

Each major subject heading in this syllabus is assigned a percentage weighting. The purpose of this is:

1. Guidance on the proportion of content allocated to each topic area.
2. Guidance on the proportion of questions in the exam.

Syllabus Area	Number of questions
1. Legal requirements relating to the use of Data.	10
2. Legal requirements related to the provision of application support services.	8
3. Structured and Unstructured Data.	4
4. Ethical Data and the implications of data use for wider society.	8
5. Security Vulnerabilities and approaches to security testing.	10
	40 Questions



CONTACT

BCS want every apprentice to have the best possible experience in their end-point assessment. Should further support be required to achieve this please contact us:

E: apprenticeships@bcs.uk

If you have any queries relating to the online assessments, please contact;
Service Delivery - eprofessional@bcs.uk

For further information please contact:

BCS
The Chartered Institute for IT
3 Newbridge Square
Swindon
SN1 1BY

T +44 (0)1793 417 445

www.bcs.org

bcs
The Chartered Institute for IT