BCS LEVEL 4 DIGITAL CORE

SYLLABUS

The Chartered Institute for IT

March 2024 v1.4

Unit Code: K/618/8039

CONTENTS

bcs
The Chartered Institute for IT

Introduction

As digital technologies continue to evolve, they become an ever more intrinsic part of our daily lives and our society. This is significantly transforming the way in which businesses operate and the requirements for today's workforce. As such there is an ever-increasing need for individuals equipped with the skills and knowledge to support the development and implementation of digital solutions within a business that deliver efficiencies and greater productivity; that enable insight through data; that provide greater security; that deliver enhanced customer experiences; and that ensure successful operations can be carried out.

This need goes beyond the basic understanding of a specific role; these individuals must also understand the business environment and the needs of their stakeholders, whilst being able to communicate and collaborate with others in diverse and cross-functional environments, to achieve a common goal.

Developing a working knowledge of the key concepts in cyber security, networks, systems and applications, data, and programming will help learners to succeed in a modern, collaborative environment.

Find out more about the BCS Level 4 Digital Modular Programme qualification in the Qualification Guide.

Qualification Suitability and Overview

There are no mandatory requirements for learners to be able to undertake this qualification, although learners will need a good standard of written English and maths. Learners must be aged 16+ to take this module.

This qualification is suitable for learners who are looking to progress in their digital careers, as well as those looking to move into a particular specialism. 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 applied knowledge, skills and behaviours to a range of scenarios.
- enable a learner to demonstrate an understanding of the key concepts across each of topic areas for digital core, understanding their impact on an organisation.
- enable a learner to progress in their career.

Learners can study this module by attending a training course provided by a BCS accredited Training Provider or through self-study.

Total Qualification Time	Guided Learning Hours	Independent Learning	Assessment Time
87 hours	50 hours	35 hours	1.5 hours

Trainer Criteria

It is recommended that to effectively deliver this certification, trainers should possess:

- 10 days' training experience or have a train the trainer qualification.
- A minimum of three years' practical experience in an IT or digitally-focussed role.

SFIA Levels

This module provides learners with the level of knowledge highlighted within the table, enabling learners to develop the skills to operate successfully at the levels of responsibility indicated.

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**

Learning Outcomes

Upon completion of the module learners will be able to demonstrate an understanding of key concepts within the following topics, as well as their implications and uses within an organisation.

- Cyber security
- Networks
- Systems and applications
- Data
- Programming

Syllabus

1. Business context and emerging technologies. (15%) (K4)

Learners will be able to:

1.1 Identify an organisation's structure, evaluating how this influences the way in which it operates.

Indicative content	Guidance
a. Hierarchical, flat, functional, matrix b. For/Not for profit organisations c. Public organisations d. Private/Public limited companies e. Sole traders f. Charities	The structure of an organisation impacts the way it operates and its legal obligations. Learners will be able to identify a given organisational structure and recall its key features and uses within an organisation, for example, reporting lines and shareholding. They will also be able to explain how different structures enable particular ways of working, for example, a matrix structure and how this enables collaboration in an agile project working environment.

1.2 Analyse and interpret an organisation's mission and vision statement.

Indicative content	Guidance
a. Purpose and direction b. Shared values c. Behaviour – inspiration, belonging d. Planning	The organisation's vision exists to provide clarity on their purpose and reason for existing, defining their long-term aspirations and their target future state. The mission describes the organisation's core values and activities, providing a sense of direction on what the organisation will do to achieve the vision. It provides guidance on how the organisation should run, and assists with current and future planning. Both should be used to provide direction and inspire employees. Learners will be able to explain why an organisation would choose to develop and share a formal mission and vision statement.

1.3 Explain the purpose of organisational and personal objectives.

Indicative content	Guidance
a. KPIs b. Alignment with vision c. Reporting d. Performance management e. Personal development f. Competitors	Objectives are created as a means to drive performance towards goals (vision, mission) in a measurable way. Key performance indicators (KPIs) are specific, quantifiable metrics that track the performance of an organisation in achieving its objectives. Providing individuals with their own objectives may increase motivation and can be a helpful tool in measuring their performance and helping them work towards a personal or professional goal.

1.4 Interpret and apply organisational policies and procedures.

Indicative content

a. IT acceptable use
b. Health and safety
c. Equality, diversity and inclusion
d. Confidentiality
e. Risk management
    - Identify
    - Analyse
    - Evaluate
    - Treat
    - Monitor and review
f. Data protection

Guidance

Organisations provide policies and procedures to ensure the safe, consistent and legal running of their business. These will naturally vary across organisations but will generally include a combination of, or take on, the topics listed. Learners will have a practical understanding of the typical policies and procedures that exist in a business, their purpose, contents, and application.

1.5 Analyse the use of new and emerging technologies in an organisational context.

Indicative content

a. The 4th Industrial Revolution
b. Digital transformation
c. Digital ecosystems
d. The benefits and use of:
    - Cloud technology
    - Mobile technology
    - Artificial intelligence
    - Robotics

Guidance

Digital transformation describes the process through which an organisation adapts and enhances its ways of operating through the adoption of digital technologies. Learners should be able to define the terms listed, and have understanding of the uses of different technologies and the benefits and challenges associated with them. They should consider the influence of the technologies on how an organisation operates and the impact on its customers.

2. Business culture in a digital environment. (10%) (K4)

Learners will be able to:

2.1 Analyse an organisation's culture and how it influences working practices.

Indicative content

a. Ethics and ethical qualities
b. Equality and diversity
c. Top-down and bottom-up
d. Change and risk approaches
e. Digital mindset

Guidance

It is commonly acknowledged that culture is a combination of personal experience and perceptions, and therefore it cannot be entirely managed by the organisation. The culture of an organisation can be seen in its values and principles and is impacted by factors such as the diversity of the workforce, the sector in which it operates and the behaviour of its employees. Learners should be able to define the term 'ethics' and understand qualities that demonstrate ethical behaviour, such as honesty, integrity, respect and compassion.

Learners should be able to discuss the impact of culture on business activity, decision-making and the organisational approach to change and risk taking, including understanding the term 'risk appetite'. They should also consider the need for an organisation to have a digital mindset in order to leverage the digital innovations that deliver efficiencies and help to gain a competitive edge in the market.

2.2 Analyse the business context for software applications, their usage and development.

Indicative content

a. SWOT, PESTLE
b. The market environment
c. Suitability of solutions
d. Sustainability
e. Scalability and future proofing

Guidance

Learners should consider the potential use of software for an organisation and assess the suitability of the software to meet the business needs in current and future landscapes. For example, will the software be fit for purpose if the business experiences rapid growth or if legal requirements change?

Learners should be able to define the terms listed, and should be encouraged to undertake an analysis of their own business environment through the use of SWOT or PESTLE analysis to identify opportunities for using different software.

---

3. The principles of cyber security. (20%) (K2)

Learners will be able to:

3.1 Explain how information and cyber security can affect society.

Indicative content	Guidance
a. Information sharing b. Theft and fraud c. Data protection d. Privacy e. Human rights	Information and cyber security have a significant impact on the way society live and work, including how our data and information is used and shared, and how our activity is monitored. Learners should be able to explain a range of ways in which society is affected.

3.2 Explain why cyber security is important to organisations.

Indicative content	Guidance
a. Protect data and intellectual property b. Legal and organisational compliance	Robust cyber security ensures that organisations can fulfil their legal obligations around processing and storing data, as well as protecting other intellectual property. Cyber security also protects the organisation's devices and networks from potential attacks or threats. Learners should understand the term, and recognise examples of organisational assets that constitute intellectual property.

3.3 Explain the importance of following organisational policies and procedures relating to information security.

Indicative content	Guidance
a. Creating vulnerabilities b. Reputational impact c. Interrupted operations d. Financial loss	Non-compliance with policies and procedures inevitably creates vulnerabilities in the organisation's systems, increasing the likelihood of threats or attacks. Such risks could impact the organisation's ability to provide a service to their customers, cause financial loss, and have a negative impact on their reputation. Learners should be able to understand and consider the risks associated with non-compliance and the value of ensuring all policies and procedures are understood and adhered to.

3.4 Explain the factors that contribute to a negative or positive cyber security environment.

Indicative content	Guidance
a. Compliance b. Training c. Maintenance	Learners should be able to understand a range of factors that can contribute to the positive or negative impact/use of cyber security. Consideration should be given to the benefits of compliance with organisational procedures, the training of users and the ongoing maintenance and testing of the systems, including the testing and roll out of patches and updates.

3.5 Identify security threats.

Indicative content	Guidance
a. Type of threat b. Potential impact c. Common themes	Learners should be able to identify and understand different types of security threat, including phishing, social engineering, malware, denial of service/distributed denial of service. Learners must recognise how these threats are presented, how/when they may occur, and what their potential impacts may be.

3.6 Describe security procedures.

Indicative content	Guidance
a. Intrinsic and extrinsic assurance b. Design and implementation standards c. Operational policy and process standards d. Penetration testing e. The OWASP Principles of Security	Within an organisation, security can take many different forms. Learners should understand the need for specific design, service and working standards, and how these contribute to security. Learners should be able to differentiate between intrinsic assurance (exploring how the system was built) and extrinsic assurance (outside factors and testing), and explain how and why testing is used as part of security procedures. They should be familiar with the OWASP Principles of Security and how these help developers build secure applications.

3.7 Explain the importance of maintaining data and program integrity by backing up the data securely and regularly.

Indicative content	Guidance
a. Avoid data loss b. Record keeping c. Disaster recovery	Regular backup of data provides a range of benefits to an organisation and individual. As well as ensuring that data can be recovered after loss or theft, backing up data helps to ensure any changes or updates are saved, and can help with reporting and audit trails if required. Learners should understand data backup best practices, such as the 3-2-1 strategy, and be able to explain how and why backup activity should be completed and the impact of doing/not doing so on the integrity of data and the organisation.

4. The principles of networks, systems and applications. (15%) (K2)

Learners will be able to:

4.1 Describe how different operating systems interact with different platforms.

Indicative content	Guidance
a. Desktop b. Portable computing e.g. laptops, tablets c. Smartphones d. Dedicated devices e.g. satnavs, fitness trackers, smart home interfaces	Learners should be aware of different platforms and operating systems available, and the impact these have on build, testing and development. Operating systems may include Android, iOS, Mac OS, Windows or simpler, bespoke OS for niche or specialist devices. Learners should be aware that all "Internet of Things" devices use an operating system.

4.2 Describe the in-built facilities found in different types of operating systems, on different platforms.

Indicative content	Guidance
a. Security features b. Communication and networking features c. Methods of input and output d. Performance e. Versatility and customisation f. Licensing models	Operating systems (OS) each have native applications, developed specifically to be used with that OS, to create the best possible user experience. Learners should understand the challenges associated with native applications, particularly their portability and compatibility across operating systems. Learners should also understand factors, such as inbuilt security, performance and licensing models, that might influence an organisation's decision to use a particular operating system.

4.3 Describe the function of different types of server.

Indicative content	Guidance
a. Intended use b. Fit for purpose	Many different types of server may be used, depending on the purpose and requirements. Learners should be able to describe the type of server and its use, including file servers, application servers, web servers, proxy servers and cloud services.

4.4 Describe the components and equipment of a network.

Indicative content

a. Hubs
b. Switches
c. Bridges
d. WAPs
e. Routers
f. Firewalls
g. Proxy servers

Guidance

Building and running a network involves a variety of hardware and software components. Learners should be familiar with the components and equipment listed and understand their purpose, role and dependencies within the network.

4.5 Explain the positives and negatives of a range of platforms.

Indicative content

a. Functionality
b. Cost
c. Ownership
d. Maintenance
e. Usability

Guidance

When selecting or reviewing a platform, consideration must be given to a range of factors, as listed. For example, how the functionality of the platform aligns with the requirements of the user, the upfront and ongoing costs versus budget, or the flexibility of open source versus the perceived security of proprietary etc.

4.6 Explain the purpose of operating systems, databases and applications.

Indicative content

a. Perform specific activity or function
b. Data lifecycle
c. Sharing data
d. Manage processes

Guidance

The use of specific databases and applications will vary across organisations, projects and teams. Learners should be able to explain the purpose and role of the items listed to complete specific tasks or processes.

4.7 Explain the use of common types of desktop applications.

Indicative content

a. Web browser
b. Productivity tools - project management software, collaboration platforms, document management systems
c. Office tools – word processor, spreadsheet, presentations
d. Social and media – social networking, audio and video streaming

Guidance

Productivity tools are designed to enhance efficiency and facilitate collaboration, whereas office tools are primarily used for creating and presenting documents. Learners should be able to describe a range of desktop applications, such as those listed, and be able to explain the purposes and common uses within an organisation or for a particular project or role. For example, a web browser may be used to explore the internet, to find and retrieve information.

4.8 Explain the key function of business application software.

Indicative content

a. Customer relationship management (CRM)
b. Finance and payroll
c. Stock and asset control
d. People
e. Security

Guidance

Learners should be aware of common types of business application software and how they are used to support different business functions and activities.

4.9 Explain the process for installing a software operating system.

Indicative content

a. System requirements
b. BIOS
c. Install, run

Guidance

Learners should understand and describe activities undertaken to install an operating system, including the order in which the activities should be completed and the purpose of each stage.

Learners should also understand the separation between the roles of the BIOS and the operating system, as well as the reasons, processes and risks associated with updating a system's BIOS.

5. The principles of using data. (15%) (K2)

Learners will be able to:

5.1 Explain types of data and their sources in an organisational context.

Indicative content	Guidance
a. Structured/unstructured b. Quantitative c. Qualitative	Learners should be able to recognise and classify data as either structured or unstructured, understanding the source and use of the data. The type of data will depend on how it was created and managed, and its purpose. Learners should also understand the differences between qualitative and quantitative data and how they might be used by an organisation.

5.2 Explain the data lifecycle.

Indicative content	Guidance
a. Create b. Store c. Use d. Archive e. Delete	All data, regardless of its subject or use, will move through the stages of the data lifecycle. This lifecycle begins as soon as data is created and covers how and where it is stored, its use(s), the point and location of archival, and eventual deletion. Learners should understand the stages of the data lifecycle, the activities associated with each stage, and the benefits of a well-implemented data lifecycle management plan.

5.3 Explain the use of big data in an organisational context.

Indicative content	Guidance
a. Decision-making b. Business intelligence c. Analytics	Within an organisation, big data can provide detailed insight into customers, products and their uses. Once processed, big data may be analysed to assist with future planning, decision-making, identifying and predicting trends, and detailed reporting. Using big data in this manner, to derive insights that inform strategic decision making and planning, is known as business intelligence (BI). Learners should be able to explain the term 'big data', and should understand the characteristics that define it, commonly referred to as the "V's" (volume, velocity, variety, veracity etc.). They should also understand and recognise common sources of big data, and the ways in which the data might be used.

5.4 Explain the key components of the data protection legislation.

Indicative content

a. UK GDPR
b. Data Protection Act 2018
c. Seven data protection principles
d. Role of the controller and data processor
e. Data protection officer

Guidance

The Data Protection Act 2018, alongside UK GDPR, provides organisations and individuals with their legal rights and obligations regarding the processing, strorage and transfer of data. Learners should understand the purpose, principles and impact of the data protection legislation listed.

The role of data controller is one who decides which data should be collected and processed, and is responsible for ensuring that these activities align with the principles of the Data Protection Act. The data processor is the entity that processes data on behalf of the controller and in accordance with their instructions.

UK GDPR mandates the appointment of a data protection officer in certain circumstances, for example for public authorities or bodies, or if the organisation is carrying out certain types of processing activities. Learners should be familiar with the role of a data protection officer and the circumstances under which appointing one is mandated by law.

6. The principles of basic programming. (12.5%) (K2)

Learners will be able to:

6.1 Describe common programming languages and paradigms.

Indicative content	Guidance
a. Functional b. Object-oriented c. Procedural	Examples of common languages include, but are not limited to, C, Python, Java, Php and C++. Learners should be able to describe each language and its use, as well as understanding the fundamental differences between functional, object-oriented and procedural paradigms.

6.2 Explain good practice when working with coding languages.

Indicative content	Guidance
a. Naming conventions b. Portability c. Comments d. Scalability e. Simplicity	The process of writing, maintaining and building on code can be improved by implementing consistent standards and ways of working. For example, ensuring that comments are added when code is being written ensures that another developer will be able to understand the code and improve its reusability in future. Learners should be able to recognise and implement best practice in these areas. Learners should also understand that portability relates to programs operating across different hardware or operating systems, while scalability is the ability of software to handle increased workloads.

6.3 Explain the need to understand the appropriate use of code with different platforms.

Indicative content	Guidance
a. Compatibility b. Infrastructure c. Project suitability	The choice of programming language can depend on a range of factors, including those listed. Learners should be able to explain the need to use a programming language which is suitable to the platform and intended use, and the overall impact of making a correct or incorrect choice.

6.4 Explain the primary elements of programming logic.

Indicative content	Guidance
a. Variables b. Conditionals c. Loops d. Input/output e. Functions	Learners must understand and be able to describe the elements listed, including how they would be used and their purpose.

7. Collaborative working in a digital environment. (12.5%) (K4)

Learners will be able to:

7.1 Analyse different stakeholders and their requirements.

Indicative content	Guidance
a. Stakeholder wheel b. Customers, partners, suppliers, regulators, employees, managers, owners, competitors c. Power/Interest Matrix	All stakeholders have a level of interest or influence in an organisation, which can impact their requirements and how they need to be managed. This can be recorded using a Power/Interest Matrix. The stakeholder wheel is a tool which can also be applied to help to identify and categorise key stakeholders into one of eight groups. The role of a stakeholder may change over time, as a business changes or project develops.

7.2 Apply communication methods required for effective working.

Indicative content	Guidance
a. Verbal/non-verbal b. Written c. Visual d. Active listening	Communication takes many forms, but all can be categorised as either verbal or non-verbal. Different forms of communication are likely to be more suitable in some scenarios than others. Verbal communication may be open to interpretation in some situations, whereas written documents may provide more clarity. Each method of communication, including active listening, should be considered in its suitability for the intended audience, timescale, resources and content.

7.3 Explain methods used to influence without authority.

Indicative content	Guidance
a. Share information and expertise b. Communication c. Empathy d. Collaboration	Learners should understand ways in which teams or individuals without authority are able to influence others in the workplace, including the application of expertise, purposeful collaboration and displaying empathy and understanding.

7.4 Explain concepts of agile working practices.

Indicative content	Guidance
a. The Agile Manifesto and the 12 agile principles b. Agile mindset c. Servant leadership d. Iterative and incremental delivery	Agile working practices provide an alternative to linear or "waterfall" ways of working. The agile principles and mindset are focused on working to provide a usable solution at each increment, and developing it through further iterations. Learners will be able to apply these concepts to a range of scenarios.

7.5 Explain the use of the systems development lifecycle.

Indicative content	Guidance
a. Feasibility b. Analysis c. Design d. Development e. Testing f. Implementation g. Maintenance	The systems development lifecycle provides structure to the management of systems, from initial feasibility and requirements identification to ongoing maintenance. Learners will have a practical understanding of the application of the systems design lifecycle and the activities undertaken at each stage for a given project or system within an organisation.

Examination Format

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

Type	40 question online test including 20 knowledge questions and 20 scenario-based questions.
Duration	90 minutes
Supervised	Yes
Open Book	No (no materials can be taken into the examination room)
Passmark	Pass - 26/40 (65%) Distinction - 34/40 (85%)
Delivery	Digital format only

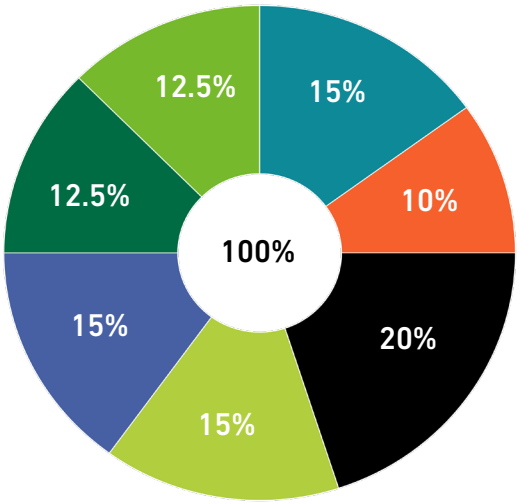
Adjustments and/or additional time can be requested in line with the BCS reasonable adjustments policy for learners with a disability, or other special considerations including English as a second language.

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 of an accredited course.
2. Guidance on the proportion of questions in the exam.

Syllabus Area	Question type	
1. Business context and emerging technologies.	Multiple choice and scenario-based multiple response.	**15%**
2. Business culture in a digital environment.		**10%**
3. The principles of cyber security.		**20%**
4. The principles of networks, systems and applications.		**15%**
5. The principles of using data.		**15%**
6. The principles of basic programming.		**12.5%**
7. Collaborative working in a digital environment.		**12.5%**
Total		**100%**



Syllabus Weighting

15% 10% 20% 15%

15% 12.5% 12.5%

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	Document creation.
Version 1.1	Updates in line with OfQual requirements.
Version 1.2	Key Topics Headers amended.
Version 1.3	Addition of OWASP Security Design Principles to criteria 3.6.
Version 1.4	Updates to indicative content and guidance, following review.

CONTACT

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

The Chartered Institute for IT