BCS LEVEL 6 PROFESSIONAL GRADUATE DIPLOMA IN IT

NETWORK INFORMATION SYSTEMS

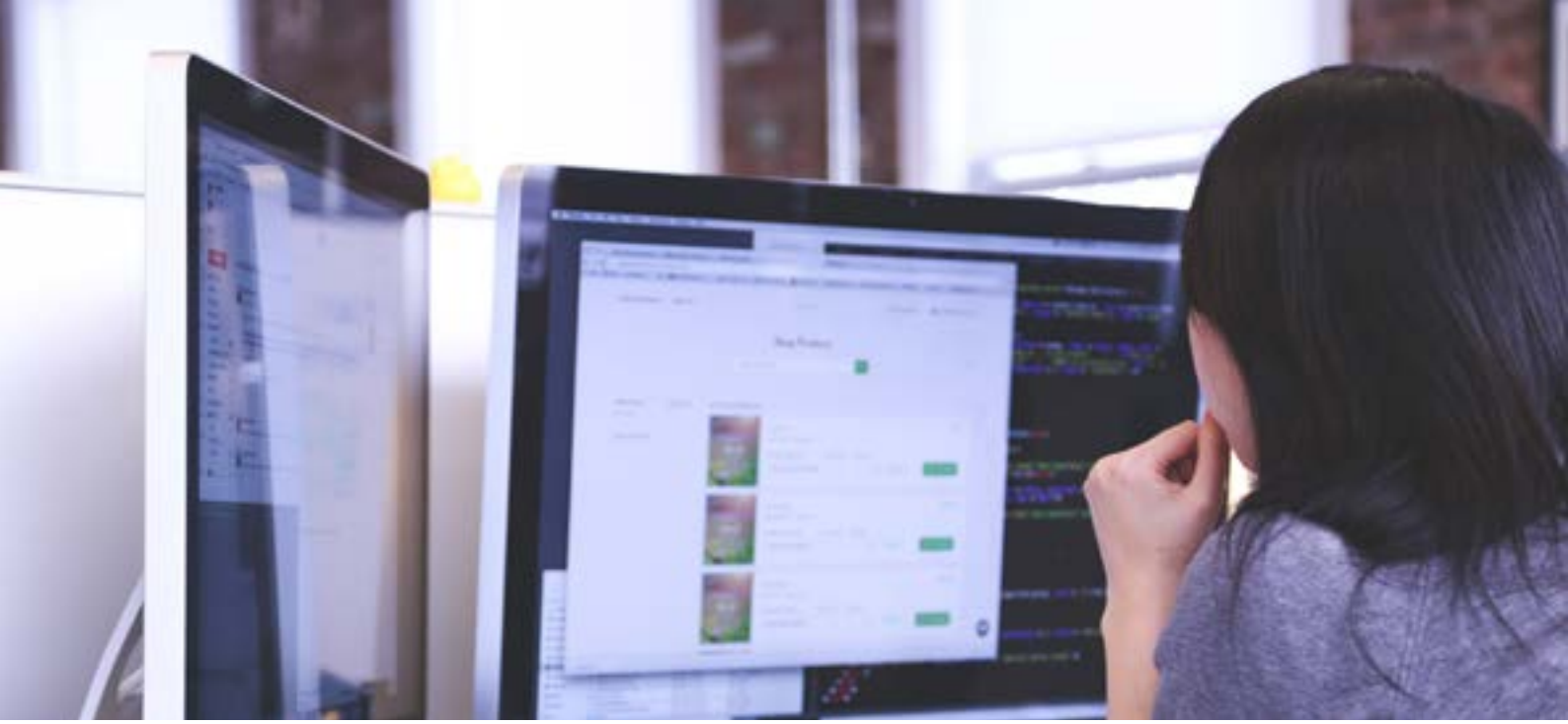
SYLLABUS

bcs The Chartered Institute for IT

September 2021 v4.0

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.

CONTENTS



Introduction

The final stage within the BCS three-stage Higher Education Qualification programme, the Level 6 Professional Graduate Diploma (PGD) enables candidates who have already achieved the Level 5 Diploma in IT to gain depth of knowledge and expertise in their field.

Our modules have been created in-line with the SFIAPlus framework and latest developments in the industry, giving you a competitive edge in the IT job market and showing your dedication to the industry. You will have the opportunity to learn about topics such as advanced database management, network information systems, web engineering and programming paradigms, as well as to build upon knowledge and skills developed during the Level 5 Diploma.
To successfully achieve the qualification, candidates need to complete:

- One core module (Professional Project in IT)
- Four optional modules

Depending on entrance conditions, completing the Level 6 PGD in IT may support entry onto a Master's degree course at selected global universities.

Network Information Systems optional module

The Network Information Systems module is an optional module that forms part of the Level 6 PGD in IT – the final stage within the BCS three-stage Higher Education Qualification programme.

Network information systems (NIS) have become ubiquitous in many parts of the world, for functions as diverse as scheduling medical treatments to managing traffic. Candidates will develop their understanding of how to propose, develop, manage and review all aspects of NIS, considering both their strategic and operational requirements.

Qualification Suitability and Overview

Candidates must have achieved the Diploma in IT or have an appropriate exemption in order to be entered for the Professional Graduate Diploma (PGD). Candidates can study for this PGD by attending a training course provided by a BCS accredited Training Provider or through self-study, although it is strongly recommended that all candidates register with an approved centre. Studying with an approved centre will deliver significant benefits.

Candidates are required to become a member of BCS, The Chartered Institute for IT, to sit and be awarded the qualifications. Candidates may apply for a four-year student membership that will support them throughout their studies.

The Level 6 PGD is suitable for professionals wishing to gain an advanced formal IT qualification, and this module may be particularly relevant for candidates who are interested in career opportunities such as network engineering, administration or architecture.

Total Qualification Time (Certificate)	Guided Learning Hours (Module)	Assessment Time (Exam)
1414 hours	**250 hours**	**Three hours**

SFIA Levels

This award provides candidates with the level of knowledge highlighted within the table, enabling candidates 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**

SFIA Plus

This syllabus has been linked to the SFIA knowledge skills and behaviours required at Level 6.

SCTY4

Explains the purpose of and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls. Performs security risk, vulnerability assessments, and business impact analysis for medium complexity information systems. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate.

ITOP4

Provides technical expertise to enable the correct application of operational procedures. Uses infrastructure management tools to determine load and performance statistics. Contributes to the planning and implementation of maintenance and installation work, including building and configuration of infrastructure components in virtualised environments. Implements agreed infrastructure changes and maintenance routines. Configures tools to automate the provisioning, testing and deployment of new and changed infrastructure. Identifies operational problems and contributes to their resolution, checking that they are managed in accordance with agreed standards and procedures. Provides reports and proposals for improvement, to specialists, users and managers.

NTDS4

Produces outline system designs and specifications, and overall architectures, topologies, configuration databases and design documentation of networks and networking technology within the organisation. Specifies user/system interfaces, including validation and error correction procedures, processing rules, access, security and audit controls. Assesses associated risks, and specifies recovery routines and contingency procedures. Translates logical designs into physical designs.

NTAS4

Maintains the network support process and checks that all requests for support are dealt with according to agreed procedures. Uses network management software and tools to investigate and diagnose network problems, collect performance statistics and create reports, working with users, other staff and suppliers as appropriate.

SCAD4

Maintains security administration processes and checks that all requests for support are dealt with according to agreed procedures. Provides guidance in defining access rights and privileges. Investigates security breaches in accordance with established procedures and recommends required actions and supports / follows up to ensure these are implemented.

Further detail around the SFIA Levels can be found at www.bcs.org/levels.

Learning Outcomes

Upon completion of this module, candidates will be able to:

- Assist in planning the development of a new networked information system in a technical environment with which they are familiar.
- Advise, within the limits of their knowledge and experience, on the suitability of information systems and network architectures for specific environments and applications.
- Give appropriate advice regarding HCI issues in relation to network information systems, with reference to other appropriate professional specialisms.
- Provide examples of both good and bad practice in networked information systems development – and justify their views by detailed analysis.
- Demonstrate knowledge of legal and moral issues relating to networked information systems. This should include the needs of security, integrity, availability, subject privacy, licensing, copyright and access management.

Syllabus

1. Advantages and disadvantages of distributed processing systems

Learners will be able to:

1.1 Explain distributed processing systems.

Indicative content	Guidance
a. Concept of distributed systems b. Examples of systems, e.g. DNS c. CAP theorem	Candidates should be able to demonstrate an understanding of what distributed systems are, as well as their benefits and challenges. They should also be able to demonstrate an understanding of the CAP theorem.

1.2 Explain distributed applications and distributed data.

Indicative content	Guidance
a. Distributed data stores b. Distributed applications c. Application of the CAP theorem	Candidates should be able to show their understanding of the difference between distributed data stores and distributed applications, and be able to identify examples of each.

1.3 Describe client/server architecture.

Indicative content	Guidance
a. Examples of client/server architecture, e.g. the web, database services, etc. b. How servers listen c. Serving multiple clients, networks and latencies	Candidates are expected to show understanding of the client/server model in practice, and understand the implication of network latency. They should also be able to apply the CAP theorem, as well as to understand challenges of systems such as distributed file systems.

2. Security, data integrity and availability of NIS

Learners will be able to:

2.1 Explain the use of back-up.

Indicative content	Guidance
a. Data integrity, e.g. the CIA triad	Candidates should be able to show an understanding of why back-up is needed and how it can be achieved over NIS. They should also demonstrate their understanding of testing back-ups and back-ups' role in NIS.

2.2 Explain the security with user access.

Indicative content	Guidance
a. Availability, e.g. the CIA triad	Candidates should understand security contexts, permissions and privileges, as well as limitations of systems such as passwords, and developments in multi-factor authentication (MFA).

2.3 Explain how to have security through control.

Indicative content	Guidance
a. ISO 27001	Candidates should understand the role of controls, although an exhaustive knowledge of all ISO 27001 controls is not required. However, candidates should be able to demonstrate an understanding what they are and why they are there, and familiarity with the controls is expected.

2.4 Explain the place of encryption in security.

Indicative content	Guidance
a. Confidentiality, e.g. the CIA triad b. Symmetric and asymmetric encryption	Candidates should be able to demonstrate an understanding of symmetric encryption and asymmetric encryption, understanding the roles of each, plus their benefits and drawbacks.

2.5 Explain the use of security certificates.

Indicative content	Guidance
a. Digital certificates b. The role of asymmetric encryption and hashing in producing them	Candidates should be able to demonstrate how certificates are used to establish authentication and understand the limitations of the scheme. They should understand the role of a certificate authority (CA) and also show their understanding of the benefit of self-signed certificates, but also what is lost.

2.6 Explain the use of digital signatures.

Indicative content	Guidance
a. Asymmetric encryption b. SSL/TLS c. Authentication d. Integrity e. Non-repudiation	Candidates should be able to show an understanding of what digital signatures are and how they may be used. They should understand the use of digital signatures in SSL/TLS but also how they are applicable more generally.

2.7 Explain the use of electronic payment systems.

Indicative content	Guidance
a. Ensuring security of payments	Candidates should be able to demonstrate an understanding of how encryption technology is used to deliver secure transfer of electronic payments.

2.8 Explain the use of ISO 27001.

Indicative content	Guidance
a. ISO 27001 certification and information security	Candidates should understand how the standard is applicable to requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS).

3. Operational network/NIS management issues

Learners will be able to:

3.1 Explain traffic modelling.

Indicative content	Guidance
a. Congestion control b. Traffic policing c. Traffic shaping	Candidates should understand the need for and concept of traffic modelling, plus how to apply traffic shaping and congestion control algorithms.

3.2 Demonstrate examples of protocols and tools used in network management.

Indicative content	Guidance
a. Simple Network Management Protocol (SNMP)	Candidates should demonstrate an understanding of SNMP, its concepts and its use in managing networks.

3.3 Explain response and performance issues.

Indicative content	Guidance
a. TCP/IP b. Burst and non-burst issues c. Latency d. Store and forward delay e. Packet loss	Candidates should be able to demonstrate an understanding of the causes of network performance issues and user application responses.

4. Human-computer interaction

Learners will be able to:

4.1 Explain the need for and requirements of good interface design.

Indicative content	Guidance
a. Web Accessibility b. Design issues	Candidates should understand the importance of good design that is accessible to all users, as well as the characteristics of poor design.

4.2 Describe human factors in system design.

Indicative content	Guidance
a. Interface between confidentiality, integrity, availability, and the human user	Candidates should demonstrate how human factors influence design, for example, in electronic payment systems, to ensure secure and user-friendly operation.

5. Local and wide area networks

Learners will be able to:

5.1 Evaluate and compare strategic and operational issues with LAN/WAN.

Indicative content	Guidance
a. For example: i. Interior and exterior routing ii. Different technologies for providing LAN and WAN	Candidates should be able to differentiate between LAN and WAN issues, understanding the strategic and operational landscape for these network types.

5.2 Demonstrate understanding of data protection.

Indicative content	Guidance
a. GDPR b. Appropriate handling of personal data	This is a key issue for the field; for example, candidates could demonstrate knowledge of events in social media and misuse of user information, among other topics.

5.3 Explain copyright, intellectual property and legislation issues.

Indicative content	Guidance
a. Including the needs of Intranet and Internet NIS development	Candidates should demonstrate an understanding of the legal and intellectual property landscape, as well as demonstrate the process of protecting intellectual property through patenting, trademarks and Digital Rights Management (DRM).

6. Local area networks

Learners will be able to:

6.1 Evaluate and compare available architectures in LAN.

Indicative content	Guidance
a. Ethernet b. WiFi c. Peer-to-peer architecture	Candidates should be able to understand the differences between various available LAN architectures.

6.2 Describe LAN performance issues.

Indicative content	Guidance
a. Latency b. Store and forward delay c. Scalability with application in LAN technology	In this area, candidates should explore key terms describing LAN performance parameters and their meaning, conveying their understanding of LAN performance issues.

6.3 Analyse bridging vs. routing in LAN.

Indicative content	Guidance
a. Comparison of Layer 2 and Layer 3 addressing b. Related performance issues c. IPv4 and IPv6 issues	Candidates should understand the difference between the ISO/OSI layer of these technologies and implementation issues related to new versions of IP.

6.4 Describe cabling infrastructure.

Indicative content	Guidance
a. Types of connections, e.g. serial, such as USB b. Types of ethernet, e.g. Twisted Pair	Candidates are expected to know the benefits and limitations of various technologies, e.g. ability to use power over ethernet, maximum length issues, and topologies.

6.5 Explain the use of hubs, switches and bridges in LAN.

Indicative content	Guidance
a. Layer 2 forwarding devices	Candidates should be able to explain the differences between various devices that operate at Layer 2 of the ISO/OSI model.

6.6 Explain traffic management in LAN.

Indicative content	Guidance
a. TCP/IP routing issues b. Reconfigurable networks c. Virtualisation of networks	Candidates should understand the operational issues of traffic management in LAN.

7. Wide area networks

Learners will be able to:

7.1 Evaluate and compare available architectures in LAN.

Indicative content	Guidance
a. Cable b. PSTN c. Wireless and satellite as broad classes of WAN structures	Candidates are only expected to understand the broad differences between these structures and the different operational characteristics of them, e.g. understanding capacity of the network architecture.

8. Messaging and information services

Learners will be able to:

8.1 Explain the use of electronic mail.

Indicative content	Guidance
a. SMTP b. IMAP and POP protocols c. MX DNS records d. Other mail software	Candidates should be able to demonstrate their understanding of the difference between POP- and IMAP-based email systems, evaluating the benefits of each approach. They should understand mail delivery and security issues, as well as the role of MX records in the DNS.

8.2 Explain the use of hubs, switches and bridges in LAN.

Indicative content	Guidance
a. The Web as a concept b. Web servers c. Client software d. HTTP and HTTPS protocols e. Three-tier architecture	Candidates should be able to demonstrate an understanding of the development and use of web services.

8.3 Explain protocols for web services.

Indicative content	Guidance
a. SOAP b. WSDL c. UDDI d. REST e. JSON	Candidates are expected to define and explain the use of these protocols to build web services.

8.4 Explain website development and management.

Indicative content	Guidance
a. HTTP b. HTTPS c. Encryption d. Content management systems e. Server hosting	Candidates should understand the use of low-level and high-level operational management of websites and hosting.

Examination Format

This module is assessed through completion of an invigilated written exam.

Type	Three written questions from a choice of five, each with equal marks
Duration	Three hours
Supervised	Yes
Open Book	No (no materials can be taken into the examination room)
Passmark	10/25 (40%)
Delivery	Paper 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.

Question Weighting

Candidates will choose three questions from a choice of five. All questions are equally weighted and worth 25 marks.

Recommended Reading

Primary texts

Title: Data communications and networking (fifth edition)
Author: B. A. Forouzan
Publisher: McGraw-Hill
Date: 2012
ISBN: 978-0073376226

Title: Business Data Communications - Infrastructure, Networking and Security (seventh edition)
Author: W. Stallings and T. Case
Publisher: Prentice Hall
Date: 2012
ISBN: 978-0133023893

Additional texts

Title: Secure Computing Magazine
Available at: https://www.scmagazine.com/ [Accessed 14 July 2021]

Using BCS Books

Accredited Training Organisations may include excerpts from BCS books in the course materials. If you wish to use excerpts from the books you will need a license from BCS. To request a license, please contact the Head of Publishing at BCS outlining the material you wish to copy and its intended use.

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 **July 2021**	Document Creation

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