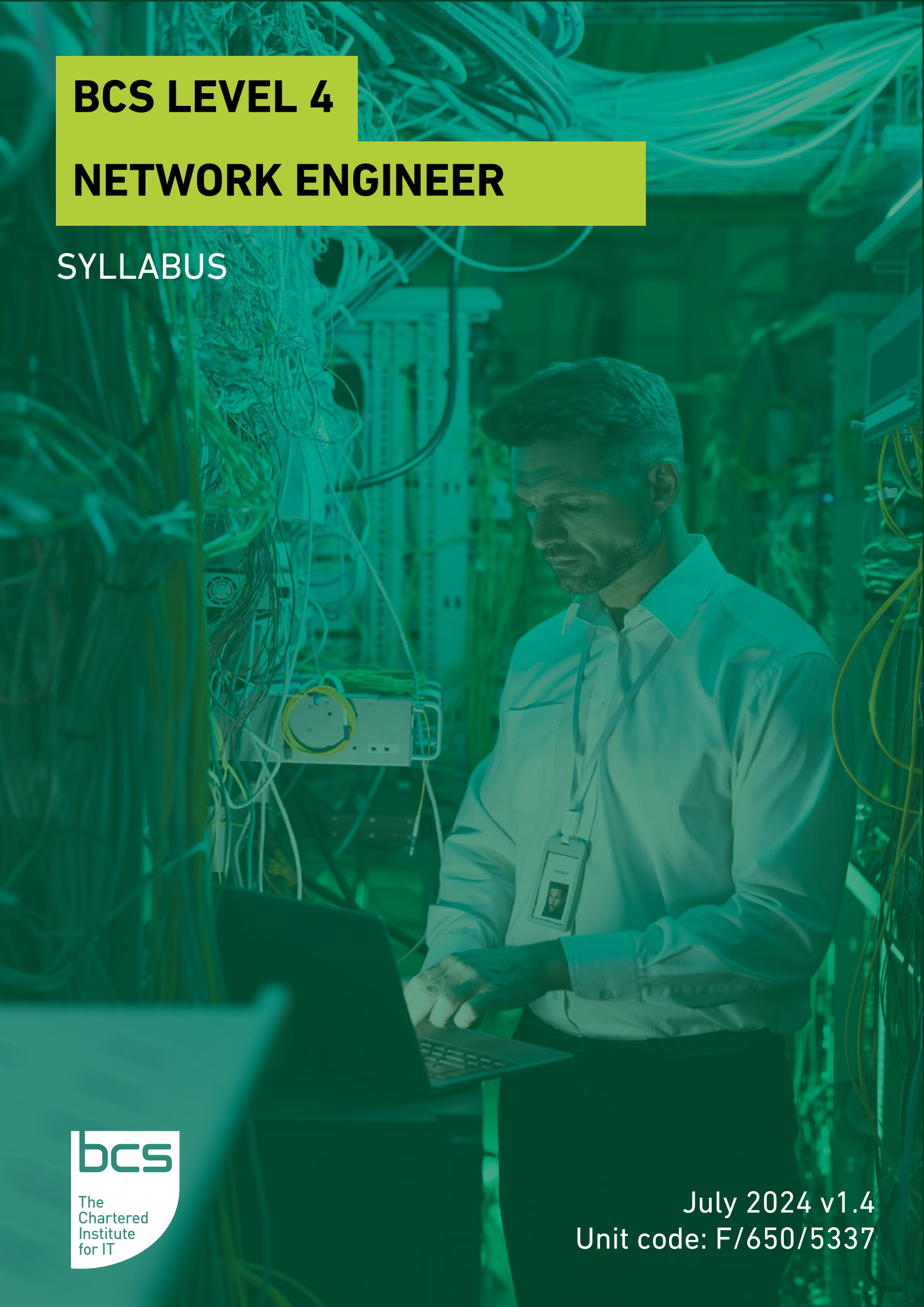
BCS LEVEL 4

NETWORK ENGINEER

SYLLABUS



The Chartered Institute for IT

July 2024 v1.4
Unit code: F/650/5337

CONTENTS

Introduction

Organisations are increasingly reliant on high performing computer networks that deliver maximum performance and availability for their staff, clients, customers and suppliers. Network engineers are essential individuals within organisations of all sizes that operate within the whole range of sectors, their primary role being the design, installation, maintenance and support of communication networks not only within the organisation but also between organisations. They will understand network configuration, cloud, network administration and monitoring tools, and will be able to give technical advice and guidance.

This level 4 module covers the key concepts, skills and tools required by anyone working within a network engineer role. It encompasses the knowledge required for carrying out tasks relating to the design, configuration and operation of computer networks.

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

Qualification Suitability and Overview

This network engineering occupational module should be undertaken as part of the BCS Level 4 Diploma - Digital Modular Programme in Network Engineering and cannot be taken as a standalone qualification. Learners must have successfully completed the exam for the BCS Level 4 Digital Core within the last 12 months in order to undertake this module.

This qualification is suitable for learners who are looking to progress their career within the network engineering field. Learners must be aged 16+ to take this module, and 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 is an occupationally focused qualification which will:

- Test a learner's ability to recall and apply knowledge in a range of scenarios
- Demonstrate a practical understanding of key concepts across the topic areas
- 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
426 hours	221 hours	203 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 a networking related 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**

SFIA Plus

This syllabus has been linked to the SFIA knowledge skills and behaviours required at level 4 for an individual working in a networking role.

KSB01 Analytical Thinking

Acquiring a proper understanding of a problem or situation by breaking it down systematically into its component parts and identifying the relationships between these parts. Selecting the appropriate method/tool to resolve the problem and reflecting critically on the result, so that what is learnt is identified and assimilated.

KSC08 Infrastructure Architecture

The frameworks and principles on which networks, systems, equipment and resources are based both on premises and cloud-based.

KSC14 Networking & Communications

The planning and management of the interaction between two or more networking systems, computers or other intelligent devices.

KSC20 Telecommunications Protocols

Rules for the inter-operation of networking components.

KSC21 Operational/Service Architecture

Knowledge of the IT/IS infrastructure and the IT applications and service processes used within own organisation, including those associated with sustainability and efficiency.

KSC27 Access Control Systems

Any tool or system which provides security access control (i.e. prevents unauthorised access to systems).

KSC52 Cloud/Virtualisation

The principles and application of cloud/ virtualisation (including ownership, responsibilities and security implications). Use of tools and systems to manage virtualised environments.

KSC60 Wi-Fi

The principles, functions and operation of WiFi components, routers, hubs and repeaters and the installation of WiFi hot-spots with appropriate use of security and encryption techniques.

KSCA1 Network Data Security

Network security and threat mitigation, including physical, electronic, firewalling, encryption, access, and authorisation; protecting data at rest and in transit; defending against viruses and malware; the impact of Big Data; and the integration of robust security controls into enterprise services and policies.

KSCA2 Infrastructure/System Security

The security threats and vulnerabilities that impact and/or emanate from system hardware, software and other infrastructure components, and relevant strategies, controls and activities to prevent, mitigate, detect and resolve security incidents affecting system hardware, software and other infrastructure components.

KSD60 Network Data Gathering Techniques

The selection, implementation and application of network data gathering methods, tools and techniques that are appropriate to the information required and the sources available.

KSC75 Safe Installation Practice

The knowledge and ability to install and maintain hardware systems to operate within their planned specification in a way that ensures they are safe to use by those authorised to work with them.

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

Learning Outcomes

Upon completion of the module, learners will be able to demonstrate a practical understanding of:

- The principles of networking and the key components of hardware and software
- How networks are designed, operated and the configuration errors that may occur
- The key features of virtualised systems, client-server operating systems and applications
- Network design considerations and the impact of errors resulting from a lack of capacity
- The causes and impact of different types of failures and errors and how to design for network resiliency
- The types of security threats that may occur, the causes and impacts of errors in security and how to mitigate them

Syllabus

1. The Principles of Networking (20%) (K3)

Learners will be able to:

1.1 Choose the appropriate components for a network.

Indicative content

a. Hardware:
   - Servers
   - Clients
   - Local and remote storage
   - Infrastructure devices (routers, switches, firewalls)
   - Media such as copper and fibre:
     - Coaxial (RG series)
     - Twisted pair (shielded, unshielded)
     - Fibre-optic
     - Common cable descriptor format
     - Understanding of ANSI/TIA 568

b. Software:
   - Operating systems
   - Protocols
   - Standards

Guidance

Learners should be able to select the appropriate hardware and software component to be used for a given purpose and justify their choice.

1.2 Compare different types of network switches and their use.

Indicative content

a. Features and designs:
   - Passive/managed
   - Stackable
   - Power over ethernet

b. Types:
   - Rack mount
   - Standalone
   - Chassis
   - Ruggedised

Guidance

Learners should be able to describe the key features of network switches, as well as understand how to manage and install them.

1.3 Identify the types of routers, their function and their key features.

Indicative content

a. Types:
   - Chassis-based
   - Standalone

b. Features:
   - Redundancy
   - Resiliency

Guidance

Learners should understand that the basic function of routers is to route packets around the network.

1.4 Compare and contrast the functions of wireless systems and select the appropriate wireless standard.

Indicative content

a. Speed
b. Frequency
c. Range
d. Security
e. Architecture

Guidance

Learners should be able to explain the different 802.11x standards (802.11a, b, g, n, ab, ac, af, ax) and implications of design, for example, which wireless devices support what standard. They are expected to select from a range of different 802.11 standards.
Learners need to differentiate between various architectural design options for wireless infrastructure and select the appropriate one.

1.5 Apply key network security devices within a network.

Indicative content

a. Firewalls:
   - Application layer firewalls
   - Network layer firewalls
   - Stateful inspection firewalls
   - Circuit level gateways
   - Next Generation Firewalls (NGFW)

b. Functions that firewalls can provide:
   - Packet filter
   - Stateful
   - Application level

c. Intrusion detection systems
d. Intrusion prevention systems

Guidance

Learners should be able to select the appropriate network security device and explain their reasoning (for example, based on the device's location within the network and its key functions). They should understand how and where to implement firewalls in the network in relation to the OSI model.

1.6 Explain the purpose of all seven layers and representative protocols at each layer within the OSI model.

Indicative content

a. Physical layer:
   - Electrical
   - Optical
   - Wireless

b. Data Link layer

c. Network layer:
   - Routing
   - Internet protocol

d. Transport layer:
   - TCP/IP protocol
   - UDP protocol

e. Session layer

f. Presentation layer

g. Application layer

Guidance

Learners should be able to explain the purpose of all layers, put them in order and describe their function. The OSI model should cover concepts, protocols and devices associated with each layer. These should be expanded as required.

At this level, learners should already understand fundamental concepts such as the difference between connection-oriented protocols (TCP) and connectionless protocols (UDP). Learners should also understand where components such as basic packet, frame and datagram fit into the model.

1.7 Describe all layers of the TCP/IP representative protocols.

Indicative content

a. Application

b. Transport

c. Network

d. Network interface

Guidance

Learners should be able to explain the purpose of all layers, put them in order and describe their function.

1.8 Explain the purpose and compare the features of IP.

Indicative content

a. IPv4

b. IPv6

Guidance

IP is the addressing scheme of computer network connectivity. With regard to IPv4, learners should understand the limitations around addressing, such as limits on the number of addresses, as well as the technologies used as work arounds for these challenges, such as network address translation (NAT). Learners should also be able to explain the differences between IPv4 and IPv6; for example, the number of addresses that can be used with IPv6 are virtually unlimited.

2. Network Design and Operation (15%) (K4)

Learners will be able to:

2.1 Use various network types, technologies and topologies.

Indicative content

a. Network topologies:
   - Physical topologies
   - Logical topologies

b. Network types:
   - LANs/VLANs
   - WANs
   - MANs
   - PANs

c. Network characteristics:
   - Reliability/fault tolerance
   - Availability
   - Security

d. Technologies*:
   - Routers
   - Switches
   - Firewalls
   - Wireless access points

*For technologies, also see LO1.2, LO1.3, LO1.4, LO1.5.

Guidance

Learners should be able to apply their knowledge of designing and implementing different types of networks.

2.2 Interpret campus network design.

Indicative content

a. Access
b. Aggregation
c. Core

Guidance

Learners should be able to describe the typical campus LAN design, following the 'hierarchy of campus network' design approach.

2.3 Apply different numbering systems.

Indicative content

a. Decimal
b. Binary
c. Hexadecimal

Guidance

Learners should be able to understand where and when to use these particular systems.

2.4 Demonstrate an ability to convert between binary and decimal.

Guidance

When designing a network using IP addressing, there are 32 binary digits: some are used by the network and the rest are used by the devices connected to the network. Learners should be able to take IP addresses given in decimal and convert them to binary, as well as calculate the host, the networking range and the appropriate subnet mask to meet the business needs.

2.5 Demonstrate an ability to calculate the number of host addresses available when given a network and a subnet mask.

Guidance

Learners should be able to calculate the numbers of hosts which can be supported.

2.6 Demonstrate an ability to calculate the necessary subnet mask when given a network diagram in order to accommodate the requirements of the network.

Guidance

Learners should be able to give the network address (or first part of the IP address) of a given number and demonstrate binary conversion to calculate how many bits it takes up or what subnet mask is to be used.

2.7 Explain the benefits of variable length subnet masking (VLSM).

Indicative content

a. More efficient use of addressing schemes
b. Routing efficiencies

Guidance

Learners should be able to explain these benefits in relation to a scenario in which they are asked to design a network.

2.8 Interpret rules and methods to facilitate data and voice communication.

Indicative content

a. Encoding
b. Formatting and encapsulation
c. TTL
d. Delivery options:
   - Unicast
   - Anycast
   - Multicast
   - Broadcast
e. Media access methods:
   - CSMA/CD
   - CSMA/CA
   - Token passing
   - FDDI
f. IEEE 802 protocol series (802.3, 802.11, 802.15, 802.16)
g. Voice over Internet Protocol (VoIP)

Guidance

Learners should understand how data is transported across a network, including details of packet structure, access method and protocols.

Learners should be aware of the amount of bandwidth VoIP requires and the fact that it should be on an untagged VLAN.

2.9 Identify the role of protocols in facilitating interoperability in network communications and use different types of routing protocols.

Indicative content

a. RIPv1
b. RIPv2
c. OSPF
d. EIGRP
e. RIPng
f. OSPFV3
g. EIGRP for IPv6

Guidance

Learners should understand the relative merits and different types of routing protocols, such as distance vector as opposed to link state, as well as some of the key functionality these protocols use, such as DUAL or Dijkstra. Learners should also have a basic understanding of the spanning tree protocol.

2.10 Use network monitoring systems to collect data for statistical analysis and forecasting.

Indicative content

a. Hardware
b. Bandwidth

Guidance

Learners should understand the tools available in networking devices as well as third party tools (e.g. Simple Network Management Protocol - SNMP) to collect and monitor relevant network data. They should apply appropriate techniques to monitor and record data in accordance with organisational specifications.

3. Servers and Virtualisation (15%) (K4)

Learners will be able to:

3.1 Describe the functions of basic components of virtualised systems.

Indicative content

a. Hypervisor (type 1 and type 2)
b. Guest
c. Hardware acceleration extensions (VT-x/AMD-V)
d. Sharing physical resources, such as memory, storage, compute (CPU)

Guidance

Learners should be able to explain the benefits of virtualisation and design considerations for implementation.

3.2 Compare the various levels of cloud service.

Indicative content

a. Infrastructure as a Service (IAAS)
b. Platform as a Service (PAAS)
c. Software as a Service (SAAS)

Guidance

Learners should understand the different services and how they may be used in a network design. They should be able to describe the similarities and differences in each, select the appropriate service in a given situation and justify their selection.

3.3 Describe the function of virtual desktop infrastructure.

Indicative content

a. Image design and support
b. User profiling
c. Security considerations
d. Network architecture design
e. Performance considerations

Guidance

Learners should be able to explain the benefits and design considerations for implementing a virtual desktop.

3.4 Compare server implementations.

Indicative content

a. Physical servers
b. Virtual servers
c. Cloud servers

Guidance

Learners should be able to identify differences between physical and virtual servers, as well as the key features of virtualisation such as host (type 1 and type 2), guest, hardware acceleration extensions (VT-x/AMD-V), sharing of physical resources such as memory, storage, compute (CPU).

Learners should be able to describe the approach taken to deliver virtual servers via a cloud-based platform.

3.5 Apply knowledge of the features of a typical client operating system.

Indicative content

a. Designed for end user
b. Includes a GUI
c. Accesses resources provided by a server
d. User applications are locally installed

Guidance

Learners should understand and use the typical client OS features, including aspects such as thin and thick clients.

3.6 Describe the features of a typical server operating system.

Indicative content

a. Shares resources to client systems
b. Stores resources centrally for easy management
c. May have a GUI and/or CLI

Guidance

Learners should be able to describe typical server OS features.

3.7 Analyse the functions of different types of network services and servers and implement the appropriate ones.

Indicative content

a. Network services:
   - Active directory (including authentication or network access server, e.g. domain controller, RADIUS)
   - DNS (domain name services)
   - DHCP (dynamic host configuration protocol)
   - GPO (group policy)
   - VPN

b. Servers:
   - Domain controller
   - File and print servers
   - Database server
   - Mail server
   - Web server

Guidance

Learners should be able to describe in detail the purpose and functions of each type of server and how they work in the network to provide key services. Learners also need to be able to decide on the appropriate server to use.

3.8 Choose the appropriate business application software based on its key functions.

Indicative content

a. General, e.g. communication via email, instant chat, VOIP, video conference
b. Sales, e.g. customer relationship management
c. Marketing, e.g. presentation and communication
d. Finance, e.g. accountancy packages
e. HR, e.g. employee record management
f. Technical support, e.g. helpdesk

Guidance

Learners should be able to describe the key types of applications running on the network, the performance considerations and any potential issues that may arise. They should be able to select the business application software appropriate to the needs of the business.

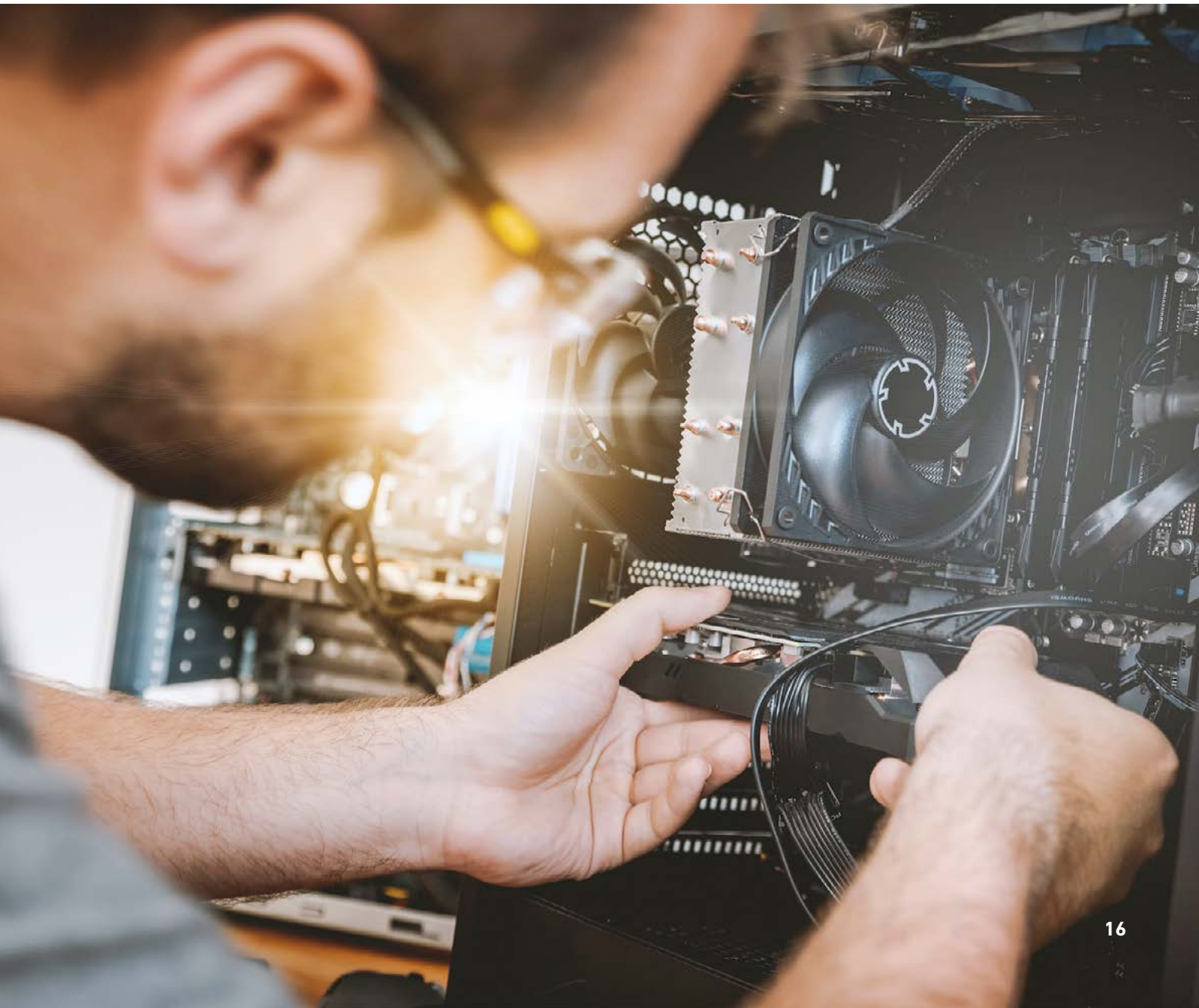
3.9 Explain the key features of middleware.

Indicative content

a. Distribute and coordinate processing across many hardware and application platforms
b. Provides a centralised location for 'business logic'
c. Provides a framework for the forwarding and queuing of transactions

Guidance

Learners should be able to explain and demonstrate how to use typical applications, including web servers, application servers and CMS.



4. Performance (15%) (K4)

Learners will be able to:

4.1 Implement design features for attaining, maintaining and optimising network performance.

Indicative content

a. Speed
b. Bandwidth
c. Application profiles
d. QoS mechanisms
e. Resource capacity
f. Eliminating single points of failure

Guidance

Learners must be aware of network design considerations for maintaining and optimising performance, including speed, bandwidth, application profiles, QoS mechanisms, and device resource capacity such as storage and memory. Performance data should be monitored and recorded in accordance with organisational specifications.

4.2 Analyse the causes of high network latency and the impact on different applications, and identify the appropriate response.

Indicative content

a. Restricted bandwidth
b. Network overload
c. Application priority
d. Distance

Guidance

High network latency jitter on time critical services and poor quality VOIP / video conferencing sessions. Learners should be able to understand how to identify network latency issues and possible options for mitigation, such as increasing bandwidth, implementing quality of service on network devices or restricting other traffic. They should be able to summarise appropriate responses to a variety of possible causes.

4.3 Analyse the causes of lack of bandwidth and identify the appropriate response.

Indicative content

a. Excessive traffic
b. Misconfigured network device(s)

Guidance

Learners should understand how to identify overall network traffic to look for causes of congestion and to analyse network device configuration for any potential issues.

4.4 Analyse the causes of lack of storage capacity and identify the appropriate response.

Indicative content

a. Poorly maintained storage
b. Insufficient trend analysis
c. Systems failures creating large data files

Guidance

Learners should be familiar with the types of issues that can be caused by storage capacity. For example, lack of maintenance and storage filling could result in the system slowing down or crashing. Neglecting to plan for future storage needs or a system failure producing large files could have a similar result.

4.5 Analyse the causes of lack of memory and identify the appropriate response.

Indicative content

a. Unexpected demand
b. Application memory leaks
c. Failure to plan

Guidance

Learners should be able to identify typical issues with memory capacity, caused by memory leaks, unexpected or unplanned increased demand. They should also be able to describe appropriate responses.

4.6 Analyse the causes of lack of compute (CPU) capacity and identify the appropriate response.

Indicative content

a. Unexpected demand
b. Failure to plan

Guidance

Learners should be able to apply appropriate responses to various causes for systems slowing down or crashing.

4.7 Use tools to automate network tasks.

Indicative content

a. Windows update service
b. MDM (mobile device management)
c. Group policy (to push out software upgrades)
d. Antivirus updates
e. Network scanning
f. Backups

Guidance

Learners should be able to select the appropriate automation tool, justify their choice, as well as implement the tool.

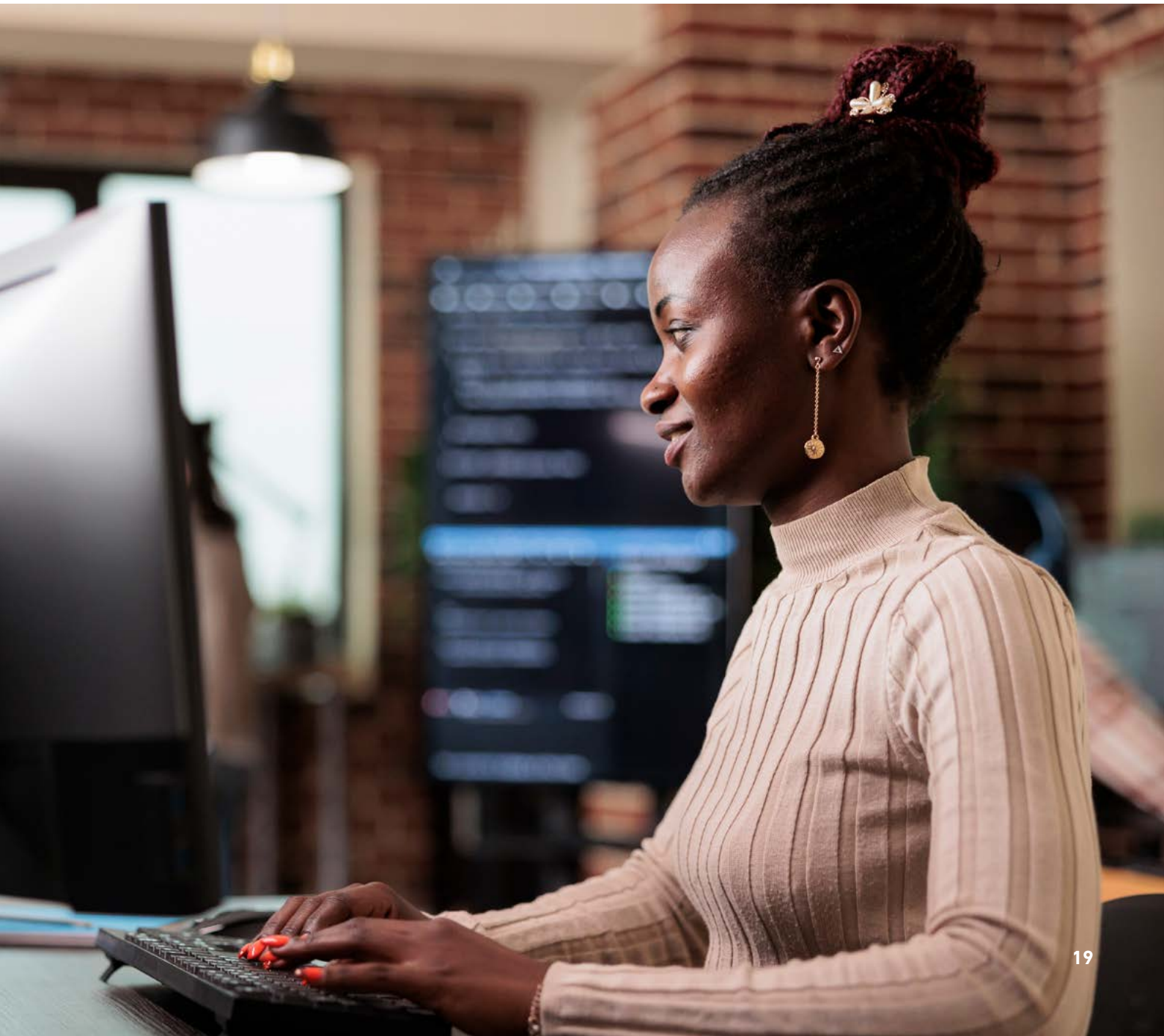
4.8 Demonstrate the ability to monitor, maintain and implement measures to improve network performance.

Indicative content

a. Preventative maintenance (e.g. routine)
b. Reactive maintenance (e.g. corrective, emergency)
c. Security maintenance
d. Business continuity and disaster recovery

Guidance

Monitoring, maintaining and implementing measures to improve network performance is crucial for ensuring a stable, secure and efficient network environment. By proactively monitoring the network, performing regular maintenance tasks and strategically applying performance improvement measures, potential issues can be prevented, and network performance as well as user experience can be enhanced. To monitor network performance, learners need to be able to use monitoring tools (e.g. WireShark, Solarwinds, PRTG).



5. Reliability and Availability (15%) (K4)

Learners will be able to:

5.1 Implement network design considerations to maintain network reliability and availability.

Indicative content

a. Individual device component redundancy
b. Individual device redundancy
c. Link level redundancy
d. Network level redundancy

Guidance

Learners should be able to independently design a network for resiliency, using a combination of hardware, software and bandwidth resources to achieve the desired levels of resiliency to failure.

5.2 Analyse the causes and impact of computer systems failure and identify the appropriate response.

Indicative content

a. Memory component failure, resulting in individual node crash
b. SSD/HDD failure, resulting in system crash and possible loss of data
c. CPU failure, resulting in intermittent system crash or failure to boot on a single node
d. Power supply, resulting in intermittent system crash or failure to boot on a single node
e. Cooling, resulting in intermittent crash or possibly permanent damage to components

Guidance

Learners should understand the impact of failure and how it can be recognised. They should follow the appropriate recovery procedure.

5.3 Analyse the causes and impact of a network failure and identify the appropriate response.

Indicative content

a. NIC failure
b. Switch failure
c. Router failure
d. Firewall failure
e. Web proxy failure
f. Incorrect cable type
g. Cabling exceeding recommended lengths and/or EMI
h. Wireless failure

Guidance

Learners should understand how failure can be recognised and its potential impact. They should follow the appropriate recovery procedure.

5.4 Analyse the causes and impact of excessive heat and identify the appropriate response.

Indicative content

a. Intermittent restarts
b. Complete component failure

Guidance

Learners should understand the impact on network devices from data centre air conditioning failure or conditions in the local environment, which may affect the multiple hardware devices adversely. They should also be able to explain the importance of maintaining an appropriate temperature and demonstrate how to do this.

5.5 Analyse the causes and impact of a lack of power and identify the appropriate response.

Indicative content

a. Blackout
b. Brownout

Guidance

Learners should consider intermittent problems, system reboots, complete loss of systems and data and configuration loss.

5.6 Analyse the causes and impact of DNS round robin and network load balancing failures and identify the appropriate response.

Indicative content

a. Misconfiguration
b. Single node failures
c. Multiple node failures
d. Failure of all nodes

Guidance

Learners should understand what load balancing is, how it is used to improve resiliency and performance of the network, the types of issues that can arise from configuration and/or link failures, and how to troubleshoot issues.

5.7 Analyse the causes and impact of locally attached storage protocol failures and identify the appropriate response.

Indicative content

a. Hardware failure

Guidance

Learners should be able to identify locally attached storage protocol failures (SATA, SCSI, SAS) which may lead to a loss of access to local disk(s) or corruption of data. They should also analyse the reasons for these failures, describe their impact, and identify an appropriate action to take.

5.8 Analyse the causes and impact of failures of RAID (0,1,5,10) and identify the appropriate response.

Indicative content

a. Loss of single or multiple disks, leading to reduced throughput or loss of data
b. Loss of RAID controller, leading to temporary or permanent loss of access to data

Guidance

Learners should understand the different RAID options, how to implement them, and their advantages and disadvantages.

5.9 Analyse the causes and impact of storage area network (SAN) failures over the Fibre Channel protocol and Fibre Channel over Ethernet (FCoE) and iSCSI, and identify the appropriate response.

Indicative content

a. Single misconfigured or failed Fibre switch, leading to increased load on remaining switches and possible reduced throughput and/or storage outage
b. Loss of all fibre switches
c. Failure of a single host bus adapter (HBA)

Guidance

Learners should be able to identify the types of failure, analyse their causes and consequences, and implement appropriate solutions.

5.10 Analyse the causes and impact of cloud storage failure and identify the appropriate response.

Indicative content

a. Router or ISP failure, leading to complete loss of access
b. TCP/IP misconfiguration, leading to inability for nodes to access storage
c. Misconfigured authentication or authorisation, leading to loss of access to cloud storage
d. Cloud service provider failure, leading to loss of access to data or loss of data

Guidance

Learners should be able to analyse the causes and consequences of cloud storage failure, understand the implications of storing data remotely, as well as describe the potential issues and resolutions. There should be a particular focus on personal and enterprise storage, such as OneDrive, SharePoint, Dropbox, Google, AWS and Microsoft Azure.

5.11 Analyse the impact of incorrectly applied configuration changes and identify the appropriate response.

Indicative content

a. Intermittent problems
b. Complete loss of function
c. Failure to boot OS

Guidance

Learners should be able to identify incorrectly applied configuration changes, understand how incorrect network configuration can create problems with expected connectivity between devices and networks, what the potential impact of this is, and how they should be repaired.

5.12 Analyse the causes and impact of IP addressing configuration errors and identify the appropriate response.

Indicative content

a. Loss of access to some or all LAN, WAN or nodes
b. Invalid IP address
c. Netmask
d. Gateway
e. DNS Server

Guidance

Learners should understand the importance of correct IP addressing and be able to troubleshoot addressing conflicts or issues with network access.

5.13 Analyse the causes and impact of VLAN configuration errors and identify the appropriate response.

Indicative content

a. Invalid VLAN tagging, leading to loss of access to nodes or lack of necessary network isolation

Guidance

Learners should understand the importance of correct VLAN tagging and be able to troubleshoot network connectivity.

5.14 Apply methodologies for patching and upgrading network elements.

Indicative content

a. Apply patches to network devices
b. Implement OS upgrades
c. Minimise downtime
d. Complete backup processes

Guidance

Learners should apply various methodologies for maintaining and upgrading the software running on network devices. All maintenance and upgrades should be carried out in accordance with organisational guidelines and policy.

5.15 Explain the use of change management processes in the production of network engineering outputs.

Indicative content

a. Organisational policy on change management
b. Change management approaches

Guidance

Network engineering outputs are the deliverables/results produced during the design, implementation and management of computer networks. These outputs can vary depending on the specific stage of the network's lifecycle and the nature of the project and include network design documents, network configurations, network diagrams, and network performance reports.

When making significant network changes, consideration must be given to the impact of these changes on the end user, security, network performance, whilst risks and disruptions (e.g. downtime) should be minimised.

Common approaches to change management in network engineering include change documentation (e.g. authorisation, for example if downtime is required), establishing designated change windows, and testing proposed changes in a lab environment before deployment. Changes to the network (e.g. network diagrams, topologies) need to be documented in the change management policy.

6. Security (20%) (K4)

Learners will be able to:

6.1 Apply measures to fix identified vulnerabilities and security threats.

Indicative content

a. Security threats:
   - Virus
   - Malware
   - DDoS attacks
   - Trojan
   - Worm
   - Spyware
   - Social engineering
   - Phishing attacks
   - Man-in-the-middle
   - DNS poisoning
   - Wireless attacks
   - Malicious users
   - Adware

b. Vulnerabilities:
   - System flaws
   - Zero-day vulnerabilities
   - Misused system features
   - User error

c. Possible installation and configuration measures:
   - Network security (including port management)
   - Firewall security rules
   - Anti-virus protection
   - Access control

Guidance

Learners should recognise different types of network security threats, vulnerabilities and design flaws through which threats can occur - for example, ports, services or code. They should be able to mitigate against these weaknesses and apply measures to repair issues whilst satisfying contractual obligations and adhering to terms set out in Service Level Agreements (SLAs). All actions taken must be recorded in accordance with organisational procedures and communicated to the relevant stakeholders in the appropriate manner.

6.2 Demonstrate understanding of security procedures, secure operation and testing of networks.

Indicative content

a. Security policy
b. Securing the perimeter
c. Physical security
d. Securing the network
e. Securing devices
f. Securing applications
g. O/S updates
h. Password policies
i. Acceptable use policy

Guidance

Learners should understand how to create and implement effective security governance for the network using the appropriate tools such as Network Access Control (NAC), whilst applying current legislation and guidelines.

6.3 Apply common methods to protect data.

Indicative content

a. File and folder permissions
b. Encryption, e.g. at rest and in flight
c. Group policy
d. Current legislation and policy

Guidance

One of the ways to protect data is to either encrypt the device the data is stored on or to encrypt the data itself. Data being transmitted across the network can also be encrypted. Learners are required to identify and use tools to manage permissions for data access and have working knowledge of relevant policies and legislation such as the Network and Information Systems (NIS) regulations.

6.4 Use testing methods and data to analyse network status and vulnerabilities.

Indicative content

a. Logging source data
b. Logging analytics
c. Penetration testing
d. Vulnerability scanning

Guidance

Learners are expected to be able to explain the importance of collecting, logging and making use of data. They should also be able to use this data to analyse network status and vulnerabilities using the appropriate monitoring systems (e.g. SIEM).

Penetration testing and vulnerability scanning both aim to enhance the security of a network, however they differ in their approaches and depth of assessment. Learners should understand the features of these methods and be able to use the appropriate one.

6.5 Analyse the causes and impact of backup failure and identify the appropriate response.

Indicative content

a. Loss of connectivity
b. Lack of space on target backup medium
c. Permissions
d. Target backup medium failure

Guidance

Learners should understand the potential issues that can affect reliable backup, as well as how to monitor and resolve these. They should also understand the relevant organisational Business Continuity (BC) and Disaster Recovery (DR) principles and their role in relation to these.

6.6 Analyse the causes and impact of malware infection and identify the appropriate response.

Indicative content

a. Lack of user knowledge
b. Lack of appropriate tools
c. Incorrectly implemented tools

Guidance

Learners should consider the impact of malware infection, such as loss of some or all data, or a reduction in work efficiency. They should be able to identify weaknesses and actions which may have led to the infection, and implement measures to prevent or resolve such incidents.

6.7 Analyse the causes and impact of poor wireless security and identify the appropriate response.

Indicative content

a. Compromising access to corporate data
b. Performance issues

Guidance

Causes may include weak encryption or poor selection of passwords, and impacts may include loss of some or all data and a reduction in work efficiency. Learners should be able to maintain wireless security and implement measures to resolve issues.

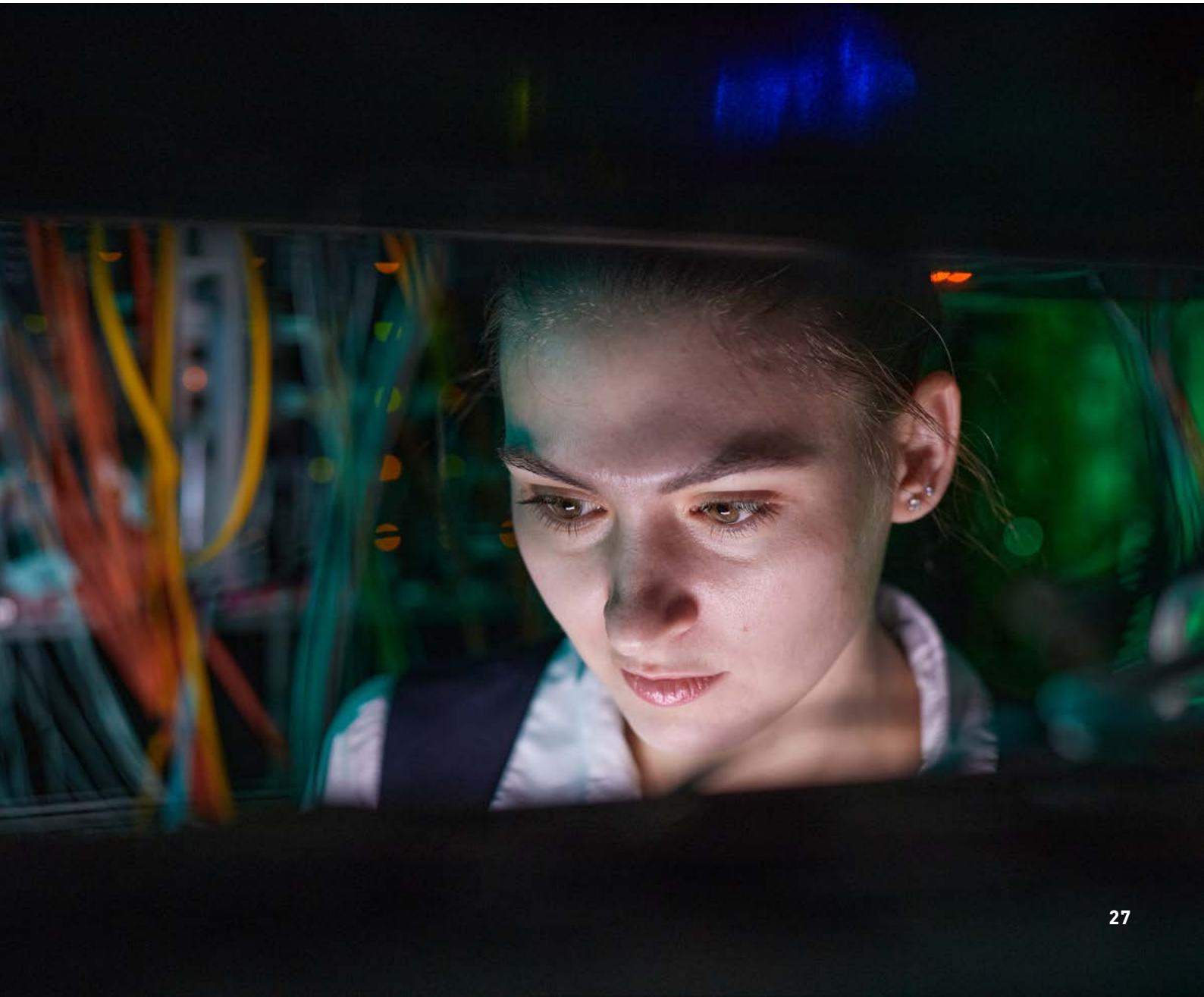
6.8 Analyse the causes and impact of failure to implement physical security.

Indicative content

a. Compromising access to corporate data
b. Performance issues

Guidance

Learners should be able to demonstrate a solid understanding of general security, such as physical access and network security.



Examination Format

This module is assessed through completion of an invigilated online exam 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:

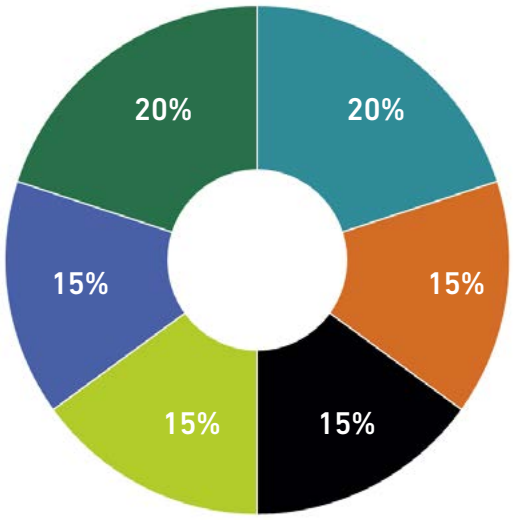
1. Guidance on the proportion of content allocated to each topic area of an accredited course.
2. Guidance on the proportion of questions in the exam.

Syllabus Area

1. The Principles of Networking	**20%**
2. Network Design and Operation	**15%**
3. Servers and Virtualisation	**15%**
4. Performance	**15%**
5. Reliability and Availability	**15%**
6. Security	**20%**
Total	**100%**

Question type

Multiple choice/ scenario-based



Syllabus Weighting

20% 15% 15% 15%

15% 20%

Recommended Reading

The following titles are suggested reading for anyone undertaking this award. Learners should be encouraged to explore other available sources.

Title: Computer Networking: A Top-Down Approach, 6th Edition
Author: Keith W. Ross and James F. Kurose
Publisher: Pearson India
Publication Date: 1 January 2017
ISBN: 9789332585492

Title: Computer Networks, 5th Edition
Author: Andrew S. Tanenbaum and David J. Wetherall
Publisher: Pearson
Publication Date: 9 January 2010
ISBN: 9332518742

Title: Data Communications and Networking
Author: Behrouz A. Forouzan
Publisher: McGraw-Hill
Publication Date: 1 July 2017
ISBN: 1259064751

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 the use to which it will be put.

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	Learning outcomes updated.
Version 1.3	Updates to the following LOs: 2.1, 2.4, 2.8, 3.4, 3.7, 4.1, 5.14, 6.1, 6.2, 6.4 New LOs added: 4.7, 4.8, 5.15
Version 1.4	Corrected qualification overview information, and figures for guided learning hours, independent learning, and total qualification time.

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