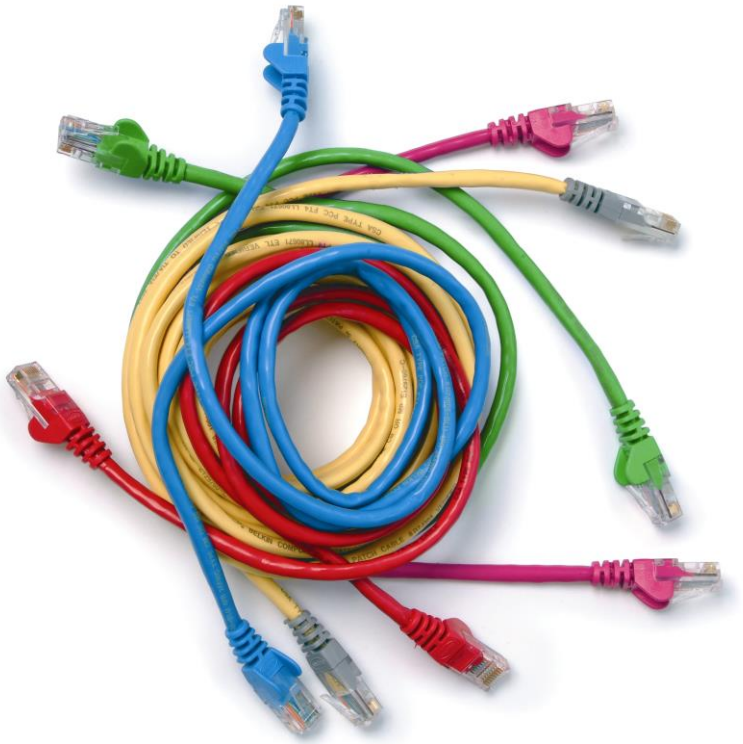
City & Guilds Diplomas in ICT Professional Competence (4520-02/03/04)

Levels 1–4 Unit Handbook for Centres
(Units 600–891)

www.cityandguilds.com
May 2011
Version 8.1 (September 2023)



This page is intentionally blank.

City & Guilds Diplomas in ICT Professional Competence (4520-02/03/04)

Levels 1–4 Unit Handbook for Centres
(Units 600–891)

Qualification title	Number	Ofqual number
City & Guilds Level 2 Diploma in ICT Professional Competence	4520-02	501/1789/0
City & Guilds Level 3 Diploma in ICT Professional Competence	4520-03	501/1788/9
City & Guilds Level 4 Diploma in ICT Professional Competence	4520-04	501/1787/7

This is page intentionally blank.

Contents

1 Introduction to this unit handbook

City & Guilds offers the following qualifications as part of its **ICT Professional Competence** qualification:

Qualification title	Number	Ofqual number
City & Guilds Level 2 Diploma in ICT Professional Competence	4520-02	501/1789/0
City & Guilds Level 3 Diploma in ICT Professional Competence	4520-03	501/1788/9
City & Guilds Level 4 Diploma in ICT Professional Competence	4520-04	501/1787/7

This unit handbook contains the units from Levels 1, 2, 3 and 4, which are part of the City & Guilds Level 2, 3 and 4 Diplomas in ICT Professional Competence.

The unit handbook should be read in conjunction with the *City & Guilds Diploma in ICT Professional Competence Qualification Handbook* (4520-02, 4520-03, 4520-04), containing the following:

- Introduction to the qualifications
- Centre requirements
- Structure of the qualifications
- Course design and delivery.

These handbooks can be downloaded from **www.cityandguilds.com**

Structure of the units

The units in these qualifications are written in a standard format and comprise the following:

- City & Guilds unit number
- Title
- Unit Accreditation Number (UAN)
- Level
- Credit value
- Statement of guided learning hours
- Unit aim
- Learning outcomes and assessment criteria.

Guidance for centres

A glossary (Appendix 1) contains a list of terms that appear in the units.

Barred combinations

Units that have a significant overlap in content are 'barred combinations'. Learners can take units that are barred and they will appear on the learner's Certificate of Unit Credit (CUC), but barred units will not both/all count towards the credit required for a qualification.

If a centre wishes to claim two (or more) barred units for a learner, they are advised to claim the unit that is most necessary to the rules of combination for the qualification and then wait until they receive the certification before they claim the other barred unit(s).

If a centre claims two (or more) barred units at the same time, they may not be recognised and therefore the learner will not be considered to have achieved the qualification.

Unit 600 Introduction to networks

UAN:	**H/507/0173**
Level:	3
Credit value:	17
GLH:	83
Aim:	This unit introduces learners to the architecture, structure, functions, components, and models of the Internet and other computer networks. It covers the principles and structure of IP addressing and the fundamentals of Ethernet concepts, media, and operations. Successful completion of the unit would enable learners to build simple LANs, perform basic configurations for routers and switches, and implement IP addressing schemes. This unit includes content from Cisco CCNA Routing and Switching curriculum. In particular, the content is relevant to the Introduction to Networks course.

Learning outcome
The learner will: 1. Understand networking within business.
Assessment criteria
The learner can: 1.1 explain how multiple networks are used in everyday life 1.2 explain how rules are used to facilitate communication 1.3 explain trends in networking that will affect the use of networks 1.4 describe how a host computer builds a message and sends it to a destination.

Learning outcome
The learner will: 2. Understand how standardisation supports interoperable end-to-end communications.
Assessment criteria
The learner can: 2.1 explain the topologies used in a network 2.2 explain the devices used in a network 2.3 explain the characteristics of a network that supports communications 2.4 explain the role of protocols in facilitating interoperability in network communications 2.5 explain the role of standards organisation in facilitating interoperability in network communications.

Learning outcome
The learner will: 3. Understand the process by which devices access resources using the TCP/IP suite.
Assessment criteria
The learner can: 3.1 explain how devices on a Local Area Network (LAN) access resources 3.2 explain how the **physical layer** supports communication across data networks (protocols and services) 3.3 explain the role of the **data link layer** in supporting communication across data networks (protocols and services) 3.4 compare media access control techniques with logical topologies used in networks 3.5 explain the role of the Address Resolution Protocol (ARP) in supporting network connectivity 3.6 explain the operation of Ethernet at the network access layer of TCP/IP within a LAN 3.7 explain how the **network layer** supports communication across data networks 3.8 explain how the **transport layer** supports communication across data networks 3.9 compare the operations of transport layer protocols in supporting end-to-end communication 3.10 explain the operation of the application layer in providing support to end-user applications 3.11 describe the features of the **application layer** 3.12 describe the operation of the application layer 3.13 describe the use of the application layer.

Range
network layer (protocols and services) **transport layer** (protocols and services) **application layer** (protocols and services)

Learning outcome
The learner will: 4. Be able to design an IP addressing scheme to provide network connectivity.
Assessment criteria
The learner can: 4.1 explain the use of IPv4 addresses to provide connectivity 4.2 calculate **IPv4 addresses** to enable end-to-end connectivity 4.3 design an IP addressing scheme to provide connectivity to end users 4.4 explain the use of IPv6 addresses to provide connectivity 4.5 explain design considerations for implementing IPv6.

Range
IPv4 addresses (network, host, broadcast)

Learning outcome
The learner will: 5. Be able to implement network connectivity between devices.
Assessment criteria
The learner can: 5.1 connect network devices with media 5.2 configure IP address parameters on devices to provide end-to-end connectivity 5.3 explain how a network of directly connected segments is configured 5.4 explain how a network of directly connected segments is verified 5.5 configure wireless on an integrated router 5.6 use testing utilities to test network connectivity.

Learning outcome
The learner will: 6. Be able to configure network access.
Assessment criteria
The learner can: 6.1 determine the devices required to route traffic 6.2 explain how routers enable end-to-end connectivity 6.3 configure a router 6.4 explain how switches in enable end-to-end connectivity 6.5 implement LAN switching to enable end-to-end connectivity 6.6 use show commands to establish a relative performance baseline for the network.

Learning outcome
The learner will: 7. Be able to configure initial Inter Network Operating System (IOS) device settings.
Assessment criteria
The learner can: 7.1 explain features of IOS software 7.2 explain functions of IOS software 7.3 configure initial setting on a network using IOS software 7.4 configure connectivity devices with device hardening features to enhance security 7.5 manage IOS configuration files to ensure device operation.

Unit 601 Routing and switching essentials

UAN:	**K/507/0174**
Level:	4
Credit value:	27
GLH:	143
Aim:	This course provides for learners an understanding of the architecture, components, and operations of routers and switches in a small network. It develops skills related to configuring a router and a switch for basic functionality. On successful completion of this unit, learners will be able to configure and troubleshoot routers and switches and resolve common issues. This unit includes content from Cisco CCNA Introduction to Networking curriculum. In particular, the content is relevant to the Routing and Switching Essentials course.

Learning outcome
The learner will: 8. Be able to configure switch ports to manage network access.
Assessment criteria
The learner can: 8.1 explain how Layer 2 switches forward data in a Local Area Network (LAN) 8.2 explain how switched networks support business 8.3 configure switch configurations 8.4 configure a switch using security best practices.

Learning outcome
The learner will: 9. Be able to implement Virtual Local Area Networks (VLANs) to logically segment networks.
Assessment criteria
The learner can: 9.1 analyse how VLANs segment broadcast domains 9.2 implement VLANs to segment a network 9.3 configure routing between VLANs 9.4 configure VLAN 9.5 configure trunking security features 9.6 implement inter-VLAN routing using Layer 3 switching to forward data 9.7 troubleshoot issues in a switched, multi-VLAN routed environment.

Learning outcome
The learner will: 10. Be able to configure routing technologies to facilitate internetwork communications.
Assessment criteria
The learner can: 10.1 explain how routers use information in data packets to make forwarding decisions 10.2 explain the function of dynamic routing protocols 10.3 configure a router for multiple directly connected networks 10.4 compare how routers learn about remote networks 10.5 analyse a **routing table** to determine information.

Range
routing table (route source, administrative distance, metric)

Learning outcome
The learner will: 11. Be able to implement static routing to enable end-to-end connectivity.
Assessment criteria
The learner can: 11.1 explain the ways in which static routes can be implemented 11.2 configure static routes to enable connectivity 11.3 troubleshoot **route configurations**.

Range
route configurations (static, default)

Learning outcome
The learner will: 12. Be able to implement Open Shortest Path First (OSPF) to enable end-to-end connectivity.
Assessment criteria
The learner can: 12.1 explain the operation of a single-area OSPF as a link-sate routing protocol that enables dynamic routing 12.2 explain the function of link-state controls 12.3 configure OSPFv2 to enable internetwork communications in a IPv4 network 12.4 configure OSPFv3 to enable internetwork communications in an IPv6 network.

Learning outcome
The learner will: 13. Be able to automate IP addressing configuration for end devices.
Assessment criteria
The learner can: 13.1 design an IP addressing scheme to provide connectivity to end users 13.2 implement DHCPv4 to provide addressing services to end-devices across multiple LANs 13.3 implement DHCPv6 to provide IP addressing services to end-devices across multiple LANs.

Learning outcome
The learner will: 14. Be able to implement Access Control Lists (ACL) to filter traffic.
Assessment criteria
The learner can: 14.1 explain the purpose of ACLs 14.2 explain the operation of ACLs 14.3 implement IPV4 **ACLs** to filter traffic 14.4 implement IPV6 ACLs to filter traffic 14.5 troubleshoot ACL implementation issues affecting end-to-end connectivity.

Range
ACLs (standard, extended)

Learning outcome
The learner will: 15. Be able to implement Network Address Translation (NAT) for IP address conservation.
Assessment criteria
The learner can: 15.1 explain NAT services in providing IPv4 address scalability 15.2 configure NAT services on the edge router to provide IPv4 address scalability 15.3 interpret device output to correct NAT implementation issues affecting end-to-end connectivity from an internal to external LAN.

Unit 602 Scaling networks

UAN:	**M/507/0175**
Level:	3
Credit value:	15
GLH:	73
Aim:	This unit develops an understanding of the architecture, components, and operations of routers and switches in large, complex networks. Learners develop understanding and skills required to configure routers and switches for advanced functionality. Successful completion of the unit would enable learners to configure and troubleshoot routers and switches and resolve common issues with OSPF, EIGRP, and STP in both IPv4 and IPv6 networks. They will also develop the knowledge and skills needed to implement a WLAN in a small-to-medium network. This unit includes content from Cisco CCNA Switching, Routing and Wireless Essentials curriculum. In particular, the content is relevant to the Scaling Networks course.

Learning outcome
The learner will: 1. Be able to configure switching hardware that facilitates network access.
Assessment criteria
The learner can: 1.1 explain the need for hierarchical network design that is scalable 1.2 select network devices to meet requirements (feature compatibility, network) 1.3 explain the purpose of the spanning tree protocol in a switched Local Area Network (LAN) environment with redundant inter-switch links 1.4 explain the operation of Per Virtual LAN Spanning Tree (PVST+) in a switched LAN environment 1.5 configure PVST+ in a switched LAN 1.6 configure Rapid PVST+ in a switched LAN 1.7 explain the operation of link aggregation in a switched LAN environment 1.8 implement link aggregation to improve performance on high-traffic switch links 1.9 verify First Hop Redundancy Protocols (FHRP) in a switched network.

Learning outcome
The learner will: 2. Be able to implement wireless Local Area Networks (LANs) to provide network access.
Assessment criteria
The learner can: 2.1 explain how standards ensure interoperability in wireless networks 2.2 explain how wireless LAN components are deployed 2.3 describe security features available in a wireless network 2.4 implement a wireless LAN using a wireless router.

Learning outcome
The learner will: 3. Be able to implement Open Shortest Path First (OSPF) to enable end-to-end connectivity.
Assessment criteria
The learner can: 3.1 explain the operation of multi-area OSPF 3.2 implement multi-area OSPF for IPV4 to enable internetwork communications 3.3 implement advanced OSPF features to enhance operation 3.4 troubleshoot singe-area OSPF configuration issues.

Learning outcome
The learner will: 4. Be able to implement Enhanced Interior Gateway Routing Protocol (EIGRP).
Assessment criteria
The learner can: 4.1 explain how the characteristics of EIGRP enable dynamic routing 4.2 explain the operation of EIGRP that enables end-to-end communication 4.3 implement EIGRP for IPv4 to enable internetwork communication 4.4 implement EIGRP for IPv6 to enable internetwork communications 4.5 implement advanced EIGRP features to enhance operations 4.6 troubleshoot EIGRP configuration issues.

Learning outcome
The learner will: 5. Be able to manage Inter Network Operating System (IOS) system image files.
Assessment criteria
The learner can: 5.1 select IOS system image files to support network requirements 5.2 configure a device to activate an upgrade IOS image.

Unit 603 Connecting networks

UAN:	**T/507/0176**
Level:	3
Credit value:	18
GLH:	91
Aim:	This unit covers the WAN technologies and network services required by converged applications in a complex network. It enables learners to understand the selection criteria of network devices and WAN technologies to meet network requirements. They will learn how to configure and troubleshoot network devices and resolve common issues with data link protocols. They will also develop the knowledge and skills needed to implement Virtual Private Network (VPN) operations in a complex network. This unit includes content from Cisco CCNA Switching, Routing and Wireless Essentials curriculum. In particular, the content is relevant to the Connecting Networks course.

Learning outcome
The learner will: 1. Understand hierarchical network design.
Assessment criteria
The learner can: 1.1 explain how a hierarchical network model is used to design networks 1.2 explain how a modular approach is used in network design 1.3 explain how business network architectures work in collaboration with enterprise architecture to allow organisations to support business.

Learning outcome
The learner will: 2. Understand Wide Area Network (WAN) access technologies for small to medium-sized networks.
Assessment criteria
The learner can: 2.1 describe WAN access technologies 2.2 select WAN access technologies to satisfy business requirements.

Learning outcome
The learner will: 3. Be able to configure a serial interface to enable WAN communication.
Assessment criteria
The learner can: 3.1 explain the operation of Point-to-Point Protocol (PPP) across a point-to-point serial link 3.2 configure PPP to enable internetwork communications 3.3 troubleshoot PPP issues that affect internetwork communications 3.4 configure High Level Data Link Control (HLDC) encapsulations on a point-to-point serial communication link to enable WAN connectivity 3.5 explain the benefits of Frame Relay 3.6 explain the operation of Frame Relay 3.7 configure Frame Relay issues that affect internetwork communications

Learning outcome
The learner will: 4. Be able to configure an Ethernet interface to enable broadband communication.
Assessment criteria
The learner can: 4.1 explain how broadband technologies support remove connectivity for business 4.2 select broadband solutions to support remote connectivity 4.3 configure a router Ethernet interface for connectivity.

Learning outcome
The learner will: 5. Be able to implement Network Address Translation (NAT) for IP conservation.
Assessment criteria
The learner can: 5.1 explain the operation of NAT services in providing IPv4 address scalability 5.2 configure NAT services on the edge router to provide IPv4 address scalability 5.3 troubleshoot NAT issues that affect internetwork communications.

Learning outcome
The learner will: 6. Be able to configure a tunnelling protocol to enable site-to-site communication.
Assessment criteria
The learner can: 6.1 explain the use of Virtual Private Networks (VPN) in securing site-to-site connectivity 6.2 configure a Generic Routing Encapsulation (GRE) to set the foundation for secure site-to-site connectivity 6.3 explain the operation of IPsec to secure VPN traffic 6.4 explain how **remote access technologies** are used to support remote connectivity.

Range
remote access technologies (Secure Socket Layer (SSL), IPsec)

Learning outcome
The learner will: 7. Be able to configure network monitoring.
Assessment criteria
The learner can: 7.1 configure Syslog to monitor network operations 7.2 configure Simple Network Management Protocol (SNMP) to monitor network operations.

Learning outcome
The learner will: 8. Be able to troubleshoot data networks.
Assessment criteria
The learner can: 8.1 determine troubleshooting approach required for network problems 8.2 troubleshoot end-to-end connectivity.

Unit 604 Practical fundamentals of ICT

UAN:	**A/507/0177**
Level:	1
Credit value:	9
GLH:	49
Aim:	This unit introduces learners to the fundamentals of personal computers. It covers basic concepts and terminology related to their operation and allows learners to develop skills to set up a workstation. It also allows learners to develop skills to install software and consider security requirements of a personal computer. This unit covers the content of CompTIA IT Fundamentals.

Learning outcome
The learner will: 1. Be able to use personal computers and their peripherals.
Assessment criteria
The learner can: 1.1 define IT terminology 1.2 identify risks associated with the **upgrading** of personal computers 1.3 identify differences between different types of **peripherals** 1.4 set up a PC workstation 1.5 use the PC to operate peripherals.

Range
upgrading (technologies and equipment) **peripherals** (connector types, monitor types, keyboard, mouse, printer)

Learning outcome
The learner will: 2. Be able to manage software installations.
Assessment criteria
The learner can: 2.1 install software 2.2 remove software 2.3 upgrade software 2.4 configure operating system 2.5 explain digital rights management 2.6 explain the function of software tools.

Learning outcome
The learner will: 3. Be able to manage files.
Assessment criteria
The learner can: 3.1 identify issues related to folder and file management 3.2 create folders 3.3 delete folders 3.4 rename folders 3.5 move folders 3.6 assign folder structure 3.7 create files 3.8 delete files 3.9 rename files 3.10 move files.

Learning outcome
The learner will: 4. Know how to manage IT security requirements.
Assessment criteria
The learner can: 4.1 recognise security risks 4.2 identify procedures to prevent security risks 4.3 recognise security breaches 4.4 identify access control methods 4.5 identify ways to resolve security breaches 4.6 identify IT related legislation.

Unit 605 Fundamentals of IT technology

UAN:	**F/507/0178**
Level:	1
Credit value:	7
GLH:	38
Aim:	This unit introduces learners to the fundamentals of computer hardware. It covers the characteristics and functions of input, storage and peripheral hardware. Learners will gain knowledge of compatibility issues and common errors and how to carry out preventative maintenance. This unit covers the content of CompTIA IT Fundamentals.

Learning outcome
The learner will: 1. Know safety issues.
Assessment criteria
The learner can: 1.1 recognise safety hazards 1.2 identify safety guidelines.

Learning outcome
The learner will: 2. Understand personal computer hardware.
Assessment criteria
The learner can: 2.1 operate computer devices 2.2 describe the characteristics of storage devices 2.3 explain the functions of storage devices 2.4 describe the characteristics of peripheral devices 2.5 explain the functions of peripheral devices 2.6 describe the characteristics of core input devices 2.7 explain the functions of core input devices.

Learning outcome
The learner will: 3. Understand hardware compatibility issues.
Assessment criteria
The learner can: 3.1 identify compatibility issues 3.2 recognise operational problems caused by hardware 3.3 use procedures to minimise risks.

Range
risks (data loss, loss of service, damage to equipment)

Learning outcome
The learner will: 4. Know how to use maintenance products.
Assessment criteria
The learner can: 4.1 identify preventative maintenance products 4.2 describe how to use maintenance products.

Unit 606 Principles and concepts of cloud computing

UAN:	**A/507/0180**
Level:	2
Credit value:	8
GLH:	40
Aim:	Learners will gain basic knowledge of the Cloud computing principles and concepts and their role in businesses. They will develop knowledge and some understanding of how cloud services are adopted by businesses. This unit covers the content of CompTIA Cloud Essentials +.

Learning outcome
The learner will: 1. Understand the characteristics of cloud services.
Assessment criteria
The learner can: 1.1 define cloud computing 1.2 define cloud computing terminology 1.3 describe the relationship between cloud computing and virtualisation 1.4 identify early examples of cloud computing 1.5 distinguish between different types of clouds.

Learning outcome
The learner will: 2. Be able to create a cloud infrastructure.
Assessment criteria
The learner can: 2.1 identify types of organisation that might benefit from cloud computing 2.2 compare cloud computing with outsourcing 2.3 explain how the characteristics of clouds and cloud services relate to business operations 2.4 explain how the characteristics of cloud computing enhance business value.

Learning outcome
The learner will: 3. Understand the technical perspectives of cloud computing.
Assessment criteria
The learner can: 3.1 describe the technical differences between private and public types of clouds 3.2 explain how the **features** of cloud computing are deployed 3.3 explain technical threats associated with cloud computing 3.4 explain how to mitigate for technical threats associated with cloud computing 3.5 describe the impact of cloud computing on application architecture 3.6 describe the impact of cloud computing on the application-development process.

Range
features (networking, automation and self-service, federation, standardisation)

Learning outcome
The learner will: 4. Understand how cloud services are adopted.
Assessment criteria
The learner can: 4.1 explain steps that lead to a successful adoption of cloud computing services 4.2 describe the skills required in an organisation adopting cloud computing 4.3 describe the critical success factors for an organisation adopting cloud computing 4.4 describe approaches for migrating applications.

Learning outcome
The learner will: 5. Understand the impact of cloud computing on organisations.
Assessment criteria
The learner can: 5.1 describe the impact cloud computing has on IT service management in an organisation 5.2 describe how IT service management in an organisation changes as a result of implementing cloud computing 5.3 describe how to explore the potential impact of cloud computing in an organisation 5.4 explain the effect of integrating cloud computing into an organisation's existing compliance risk and regulatory framework 5.5 explain the implications of direct cost for IT departments 5.6 explain the implications of cost allocations for IT departments 5.7 explain how to maintain strategic flexibility for information communication technology.

Unit 607 ICT fundamentals

UAN:	**J/507/8508**
Level:	2
Credit value:	20
GLH:	111
Aim:	The unit addresses a wide range of topics that introduce learners to the fundamental knowledge and skills of an entry-level IT professional including networking, security, virtualisation and desktop imaging and deployment. These include the ability to assemble components based on customer requirements, install, configure and maintain devices, PCs and software for end users and the ability to safely diagnose, resolve and document common hardware and software issues. Learners will also develop the skills needed to provide appropriate customer support. This unit covers the content of CompTIA A+ - both parts.

Learning outcome
The learner will: 1. Understand application security.
Assessment criteria
The learner can: 1.1 describe types of personal computer systems 1.2 state computer hardware components 1.3 state computer software components 1.4 describe hardware configurations for task-specific computers 1.5 describe the purpose of tools used with personal computer components 1.6 describe the purpose of software used with personal computer components.

Learning outcome
The learner will: 2. Be able to assemble a desktop computer to meet requirements.
Assessment criteria
The learner can: 2.1 explain the features of safe working conditions 2.2 assemble computer 2.3 boot the computer 2.4 configure components in a computer system to meet a customer's requirements 2.5 upgrade components in a computer system to meet a customer's requirements.

Learning outcome
The learner will: 3. Be able to use preventative maintenance techniques.
Assessment criteria
The learner can: 3.1 describe the benefits of preventive maintenance for personal computers 3.2 identify preventive maintenance techniques for operating systems 3.3 apply preventive maintenance techniques for operating systems.

Learning outcome
The learner will: 4. Be able to install operating systems.
Assessment criteria
The learner can: 4.1 explain the purpose of operating systems 4.2 explain client-side virtualization 4.3 use tools to perform specific tasks within a Graphic User Interface (GUI) 4.4 install operating systems.

Learning outcome
The learner will: 5. Know networks and networking technologies.
Assessment criteria
The learner can: 5.1 describe types of networks 5.2 describe networking concepts 5.3 describe networking technologies 5.4 describe physical components of a network 5.5 describe network topologies 5.6 describe Ethernet standards 5.7 identify technologies used to establish connectivity 5.8 identify preventive maintenance techniques used for networks.

Learning outcome
The learner will: 6. Understand the components of a basic laptop.
Assessment criteria
The learner can: 6.1 describe the purpose of laptop features 6.2 describe laptop display components 6.3 describe how to configure laptop power settings 6.4 describe laptop wireless communication technologies 6.5 describe the installation of laptop components 6.6 describe the removal of laptop components 6.7 identify preventive maintenance techniques for laptops.

Learning outcome
The learner will: 7. Understand the capabilities of mobile devices.
Assessment criteria
The learner can: 7.1 explain mobile device hardware 7.2 describe the features of mobile operating systems 7.3 compare methods for securing mobile devices.

Learning outcome
The learner will: 8. Be able to network computers and mobile devices.
Assessment criteria
The learner can: 8.1 establish basic network connectivity 8.2 configure email for a mobile device 8.3 connect a computer to a network 8.4 apply preventive maintenance techniques on a network.

Learning outcome
The learner will: 9. Be able to configure printers.
Assessment criteria
The learner can: 9.1 describe the features that are common to most printers 9.2 describe different types of printers 9.3 describe printer sharing procedures 9.4 share a printer 9.5 describe preventive maintenance techniques for a printer 9.6 install a printer 9.7 configure a printer.

Learning outcome
The learner will: 10. Know security requirements.
Assessment criteria
The learner can: 10.1 describe security threats 10.2 identify security procedures 10.3 identify preventive maintenance techniques for security.

Learning outcome
The learner will: 11. Understand the roles and responsibilities of the IT professional.
Assessment criteria
The learner can: 11.1 explain why good communication skills are a critical part of IT work 11.2 explain legal and ethical issues that arise in the IT industry 11.3 explain behaviours required in response to legal and ethical issues.

Learning outcome
The learner will: 12. Be able to troubleshoot problems.
Assessment criteria
The learner can: 12.1 identify the steps of the troubleshooting process 12.2 troubleshoot computer components and peripherals 12.3 troubleshoot operating systems 12.4 troubleshoot networks 12.5 troubleshoot laptops 12.6 troubleshoot printers 12.7 troubleshoot mobile devices 12.8 troubleshoot security.

Unit 608 Fundamentals of Linux based operating systems

UAN:	**R/507/0184**
Level:	3
Credit value:	7
GLH:	40
Aim:	This unit has been designed to help a learner build an understanding and skills needed to work with Linux in these topics: commands, system architecture, file system hierarchy, installation and package management. On successful completion of this unit a learner will be able to perform straightforward administrative tasks including executing backup and restore and shutdown and reboot. This unit is linked to the CompTIA Linux+ part 1.

Learning outcome
The learner will: 1. Be able to operate Linux based operating systems.
Assessment criteria
The learner can: 1.1 determine hardware settings 1.2 configure hardware settings 1.3 boot the system 1.4 change run levels 1.5 shut down the system 1.6 reboot the system.

Learning outcome
The learner will: 2. Be able to use package management.
Assessment criteria
The learner can: 2.1 design hard disk layout 2.2 install a boot manager 2.3 manage shared libraries 2.4 use package management.

Learning outcome
The learner will: 3. Be able to use Linux based operating system commands.
Assessment criteria
The learner can: 3.1 use shell commands 3.2 process text streams using filters 3.3 perform file management 3.4 use pipes 3.5 use streams 3.6 use redirects 3.7 create processes 3.8 monitor processes 3.9 kill processes 3.10 modify process execution priorities 3.11 search text files using regular expressions 3.12 perform basic file editing operations.

Learning outcome
The learner will: 4. Be able to manage files.
Assessment criteria
The learner can: 4.1 create file systems 4.2 create partitions 4.3 maintain the integrity of file systems 4.4 control file systems 4.5 manage disk quotas 4.6 manage file permissions 4.7 create links 4.8 modify links 4.9 locate files.

Unit 609 Implementing and maintaining cloud technologies and infrastructure

UAN:	**Y/507/0185**
Level:	3
Credit value:	10
GLH:	50
Aim:	This unit develops in learners the knowledge and skills required to understand standard Cloud terminologies and methodologies and to implement, maintain, and deliver cloud technologies and infrastructures. Learners will develop an understanding of aspects of IT security and use of industry best practices related to cloud implementations and the application of virtualization. It is recommended that learners have prior learning related to cloud technologies or have experience of working in a networking role. Familiarity with any major hypervisor technologies for server virtualisation, would also be helpful. This unit covers the content of CompTIA Cloud+.

Learning outcome
The learner will: 1. Understand cloud concepts.
Assessment criteria
The learner can: 1.1 compare cloud services 1.2 compare cloud delivery models 1.3 summarise cloud characteristics 1.4 define cloud terminology 1.5 explain object storage concepts.

Learning outcome
The learner will: 2. Be able to create a cloud infrastructure.
Assessment criteria
The learner can: 2.1 explain the differences between hypervisor types 2.2 compare virtual components used to construct a cloud environment 2.3 explain the benefits of virtualised cloud environment 2.4 compare storage technologies 2.5 explain storage configuration concepts 2.6 explain the benefits offered by network optimisation 2.7 explain cloud network **infrastructure** 2.8 explain **hardware** used to enable virtual environments 2.9 configure storage provision 2.10 configure network for cloud services 2.11 troubleshoot network connectivity issues.

Range
infrastructure (protocols, ports, topologies) **hardware** (resources, features)

Learning outcome
The learner will: 3. Be able to manage networks associated with cloud computing.
Assessment criteria
The learner can: 3.1 explain how **security** is implemented in networks associated with cloud computing 3.2 compare encryption technologies 3.3 compare encryption methods 3.4 identify access control methods 3.5 implement resource monitoring techniques 3.6 allocate **resources** 3.7 implement **hardening techniques** 3.8 use remote access tools 3.9 compare **disaster recovery** 3.10 describe situations which would impact on the availability of the cloud 3.11 describe solutions to meet availability requirements.

Range
security (network, storage) **resources** (physical, virtual) **hardening techniques** (guest and host) **disaster recovery** (methods, concepts)

Learning outcome
The learner will: 4. Be able to undertake systems management.
Assessment criteria
The learner can: 4.1 explain **cloud systems management** 4.2 explain the factors that affect **system performance** 4.3 test cloud services deployment 4.4 diagnose physical host performance issues 4.5 optimise physical host performance.

Range
cloud systems management (procedures, policies) **system performance** (relating to host, relating to guest)

Unit 610 Configure and manage Linux based operating systems

UAN:	**R/507/0198**
Level:	3
Credit value:	12
GLH:	71
Aim:	This unit relates to the Linux operating system. It develops in learners the skills needed to work at a junior level as a Linux administrator. This includes shells, scripting and data management, performing straightforward administrative tasks including managing user and group accounts and securing data. Learners will gain knowledge of networking fundamentals and how to connect a workstation to a LAN or a stand-alone PC via a modem to the Internet. Learners are advised to take this unit together with Fundamentals of Linux Based Operating Systems. This unit covers the content of CompTIA Linux+.

Learning outcome
The learner will: 1. Be able to use shell scripting.
Assessment criteria
The learner can: 1.1 customise the shell environment 1.2 use the shell environment 1.3 write simple scripts 1.4 customise simple scripts 1.5 use Structured Query Language (SQL) commands.

Learning outcome
The learner will: 2. Be able to configure a user interface.
Assessment criteria
The learner can: 2.1 install a user interface 2.2 configure a user interface 2.3 setup a display manager 2.4 configure accessibility.

Learning outcome
The learner will: 3. Be able to administer systems.
Assessment criteria
The learner can: 3.1 manage user and group accounts 3.2 manage account system files 3.3 schedule system administration tasks 3.4 configure localisation 3.5 configure internationalisation **guidance** translations/language.

Learning outcome
The learner will: 4. Be able to manage system services.
Assessment criteria
The learner can: 4.1 maintain system time 4.2 implement system logging 4.3 configure Mail Transfer Agent (MTA) 4.4 manage printers.

Learning outcome
The learner will: 5. Be able to configure networks.
Assessment criteria
The learner can: 5.1 describe network masks 5.2 compare private and public IP addresses 5.3 set a default route 5.4 identify services related to **ports** 5.5 describe differences between UDP, TCP and ICMP 5.6 describe differences between IPv4 and IPv6 5.7 configure network interfaces 5.8 troubleshoot networks 5.9 configure client-side Domain Name Services (DNS).

Range
ports (20, 21, 22, 23, 25, 53, 80,110, 119, 139, 143, 161, 443, 465, 993, 995)

Learning outcome
The learner will: 6. Be able to secure networks.
Assessment criteria
The learner can: 6.1 maintain network security 6.2 setup host security 6.3 secure data with encryption.

Unit 611 Implement and manage a network

UAN:	**F/507/0200**
Level:	3
Credit value:	10
GLH:	58
Aim:	Through this unit, learners will gain theoretical understanding of networking concepts and procedures for implementing and managing networks. They will develop skills needed to implement a defined network architecture with basic network security. On successful completion of this unit, learners should be able to configure, maintain and troubleshoot network devices using appropriate network tools. They will be able to make basic solution recommendation, analyse network traffic and be familiar with common protocols and media types. It is recommended that learners have achieved a qualification related to IT fundamentals or have some experience of working with networks. This unit covers the content of CompTIA Network+.

Learning outcome
The learner will: 1. Understand networking concepts.
Assessment criteria
The learner can: 1.1 compare layers of OSI with layers of TCP/IP models 1.2 identify the OSI model layer that is associated with different **services** 1.3 explain the purpose IP addressing 1.4 explain the properties of IP addressing 1.5 explain the purpose of routing and switching 1.6 explain the properties of routing and switching 1.7 identify default ports 1.8 explain the function of networking protocols 1.9 summarise Domain Naming Service (DNS) **concepts** 1.10 identify virtual network components 1.11 explain the purpose of Dynamic Host Control Protocol (DHCP) 1.12 explain the properties of DHCP.

Range
services (applications, devices and protocols **concepts** (DNS servers, DNS records, dynamic DNS)

Learning outcome
The learner will: 2. Be able to implement networks.
Assessment criteria
The learner can: 2.1 configure routers and switches 2.2 configure a wireless network 2.3 troubleshoot wireless problems 2.4 troubleshoot router and switch problems 2.5 plan a Small Office Home Office (SOHO) network 2.6 implement a SOHO network.

Learning outcome
The learner will: 3. Understand network infrastructure.
Assessment criteria
The learner can: 3.1 match standard connector types to associated network media 3.2 compare wireless standards 3.3 compare Wide Area Network (WAN) technologies 3.4 describe network topologies 3.5 compare Local Area Network (LAN) technologies 3.6 identify components of wiring distribution.

Learning outcome
The learner will: 4. Be able to manage networks.
Assessment criteria
The learner can: 4.1 explain the features of network technologies 4.2 describe a network troubleshooting methodology 4.3 troubleshoot connectivity issues 4.4 use network monitoring resources 4.5 describe the purpose of configuration management documentation 4.6 explain methods of network performance optimisation.

Learning outcome
The learner will: 5. Be able to secure networks.
Assessment criteria
The learner can: 5.1 explain threats and vulnerabilities of networks 5.2 explain methods of user authentication 5.3 describe types of network security technologies 5.4 describe types of network security methods 5.5 explain how network threats and vulnerabilities are mitigated 5.6 implement wireless security measures 5.7 configure a basic firewall.

Unit 611 Implement and manage a network

Supporting information

Evidence requirements

For 4.3 you are required to use hardware tools and software tools

Unit 612 Securing ICT systems and networks

UAN:	**D/507/0219**
Level:	3
Credit value:	9
GLH:	51
Aim:	Learners will gain theoretical understanding of concepts and procedures for securing both ICT systems and networks. They will learn to identify risk and how to participate in risk mitigation activities, provide infrastructure, application, operational and information security and apply security controls to maintain confidentiality, integrity and availability. In addition, learners will gain knowledge of applicable policies, laws and regulations and the implications of these to their activities. This unit is of most benefit to individuals with prior learning related to IT security or experience of working in IT administration. This unit is linked to the CompTIA Security+ Exam.

Learning outcome
The learner will: 1. Be able to implement network security.
Assessment criteria
The learner can: 1.1 implement security **configuration parameters** 1.2 use network **administration principles** 1.3 explain **network design** 1.4 implement common protocols 1.5 implement common services 1.6 troubleshoot security issues related to wireless networking.

Range
configuration parameters (on network devices, on other technologies) **administration principles** (rule-based management, firewall rules, VLAN management, secure router configuration, access control lists, port security, 802.1x, floor guards, loop protection, implicit deny, prevent network bridging by network separation, log analysis) **network design** (elements, components)

Learning outcome
The learner will: 2. Be able implement operational security in an ICT environment.
Assessment criteria
The learner can: 2.1 explain the importance of risk related concepts 2.2 summarise the security implications of integrating systems with third parties 2.3 implement risk mitigation strategies 2.4 implement forensic procedures 2.5 summarise incident response procedures 2.6 explain the importance of security awareness and training 2.7 explain physical security 2.8 explain **environmental controls** 2.9 summarise risk management best practices 2.10 select controls to meet security goals.

Range
environmental controls (HVAC, fire suppression, EMI shielding, hot and cold aisles, environmental monitoring, temperature and humidity controls, video monitoring)

Learning outcome
The learner will: 3. Be able to discover threats and vulnerabilities.
Assessment criteria
The learner can: 3.1 explain types of malware 3.2 explain types of attacks 3.3 summarise social engineering attacks 3.4 summarise effectiveness of social engineering attacks 3.5 select mitigation and deterrent techniques 3.6 use techniques to discover security threats and vulnerabilities 3.7 compare the proper use of penetration testing and vulnerability scanning.

Learning outcome
The learner will: 4. Be able to implement data host security.
Assessment criteria
The learner can: 4.1 explain the importance of application security controls 4.2 summarise **mobile security** 4.3 select solution to establish host security 4.4 implement controls to ensure data security 4.5 compare measures for mitigating security risks in static environments.

Range
mobile security (concepts and technologies).

Learning outcome
The learner will: 5. Be able to configure access control.
Assessment criteria
The learner can: 5.1 explain function of authentication services 5.2 select access control method to meet requirements 5.3 configure account management security controls.

Learning outcome
The learner will: 6. Be able to implement cryptography.
Assessment criteria
The learner can: 6.1 use cryptography techniques 6.2 use cryptographic methods 6.3 use Public Key **Infrastructure** (PKI).

Range
infrastructure (certificate management and associated components)

Unit 613 Install and configure a server

UAN:	**Y/507/0221**
Level:	3
Credit value:	9
GLH:	48
Aim:	This unit develops in learners the knowledge and skills required to build, maintain, troubleshoot and support server hardware and software technologies. Successful completion of the unit will enable learners to identify environmental issues; understand and comply with disaster recovery and security procedures and be familiar with industry terminology and concepts. This unit covers the content for CompTIA Server+.

Learning outcome
The learner will: 1. Be able to install system hardware.
Assessment criteria
The learner can: 1.1 explain the importance of a Hardware Compatibility List (HCL) 1.2 select **hardware components** 1.3 install hardware components into a server 1.4 configure firmware.

Range
hardware components (system boards, chassis, memory, processors, expansion cards)

Learning outcome
The learner will: 2. Be able to implement Network Operating System (NOS) software.
Assessment criteria
The learner can: 2.1 explain features of NOS security software 2.2 explain the interaction of server roles 2.3 describe **server virtualisation** 2.4 install NOS 2.5 deploy NOS 2.6 configure NOS 2.7 update NOS 2.8 implement NOS management features 2.9 select controls to meet security goals.

Range
server virtualisation (concepts, features, considerations)

Learning outcome
The learner will: 3. Be able to configure storage.
Assessment criteria
The learner can: 3.1 describe features of Redundant Array of Independent Disks (RAID) technologies 3.2 describe benefits of RAID technologies 3.3 select a RAID level 3.4 configure internal storage technologies 3.5 explain the purpose of external storage technologies.

Learning outcome
The learner will: 4. Be able to implement server access.
Assessment criteria
The learner can: 4.1 describe **elements** of networking essentials 4.2 create **system information** 4.3 utilise system information 4.4 maintain system information 4.5 determine a physical environment for a server location 4.6 describe physical security measures for a server location 4.7 describe methods of server access 4.8 implement server access 4.9 configure server access.

Range
elements (TCP/IP, Ethernet, VPN, VLAN, DMZ) **system information** (documentation, diagrams and procedures)

Learning outcome
The learner will: 5. Be able to implement disaster recovery.
Assessment criteria
The learner can: 5.1 compare backup and restoration methodologies 5.2 compare backup and restoration media types 5.3 compare types of replication methods 5.4 explain data retention and destruction concepts 5.5 implement the steps of a recovery plan.

Learning outcome
The learner will: 6. Be able to troubleshoot server problems.
Assessment criteria
The learner can: 6.1 explain troubleshooting methodologies 6.2 diagnose network problems 6.3 troubleshoot hardware problems 6.4 troubleshoot software problems 6.5 troubleshoot storage problems.

Unit 614 Implement and manage a mobile computing environment

UAN:	**K/507/0224**
Level:	3
Credit value:	8
GLH:	47
Aim:	This unit enables learners to develop the knowledge and skills required to understand and research capabilities of mobile devices and features of over-the-air technologies. Successful learners will also develop the skills needed to deploy, integrate, support and manage a mobile environment ensuring proper security measures are implemented for devices and platforms while maintaining usability. It is recommended that learners taking this unit have prior learning related to networking or have experience of working in IT administration.

Learning outcome
The learner will: 1. Be able to implement over-the-air technologies.
Assessment criteria
The learner can: 1.1 compare cellular technologies 1.2 compare Radio Frequency (RF) principles 1.3 compare RF functionality 1.4 interpret site survey for over the air communication issues 1.5 configure WiFi client technologies.

Learning outcome
The learner will: 2. Understand network infrastructure.
Assessment criteria
The learner can: 2.1 compare physical and **logical infrastructure** 2.2 describe network ports associated with mobile devices 2.3 describe network protocols associated with mobile devices 2.4 explain the technologies used for negotiating wireless to wired networks 2.5 explain the layers of the OSI model 2.6 explain disaster recovery principles 2.7 explain how disaster recovery affects mobile devices.

Range
logical infrastructure (technologies, protocols)

Learning outcome
The learner will: 3. Be able to manage mobiles devices.
Assessment criteria
The learner can: 3.1 explain policies required to certify device capabilities 3.2 compare mobility solutions to enterprise requirements 3.3 configure mobile solutions to meet requirements 3.4 implement **mobile devices** 3.5 describe emerging technologies in mobile computing 3.6 configure mobile applications 3.7 deploy mobile applications.

Range
mobile devices (procedures, operations)

Learning outcome
The learner will: 4. Understand mobile security issues.
Assessment criteria
The learner can: 4.1 identify encryption methods for securing mobile environments 4.2 configure access control on mobile devices 4.3 explain techniques used to address security requirements 4.4 explain how risks and threats to the mobile ecosystem are mitigated 4.5 implement **data integrity** on mobile devices 4.6 execute incident response steps.

Range
data integrity (device backup, data recovery and data segregation)

Learning outcome
The learner will: 5. Be able to troubleshoot mobile problems.
Assessment criteria
The learner can: 5.1 troubleshoot device problems 5.2 troubleshoot application problems 5.3 troubleshoot over-the-air connectivity problems 5.4 troubleshoot security problems 5.5 implement the steps of a recovery plan.

Unit 615 Developing security for mobile apps on iOS

UAN:	**J/507/0229**
Level:	3
Credit value:	14
GLH:	77
Aim:	This unit is for those with experience of app development and familiarity with the iOS SDK and principles of secure application development. It will develop learners' knowledge of the fundamental principles of application security, the security model of iOS devices, Web services security model and vulnerabilities and common implementations of cryptography. Learners will develop skills needed to develop moderately complex applications using the iOS SDK, use the security features of the iOS operating system and APIs, implement secure coding techniques and harden an application against attack to levels appropriate for the risk model of the application.

Learning outcome
The learner will: 1. Understand application security.
Assessment criteria
The learner can: 1.1 identify legislation for secure mobile development 1.2 describe security risks for mobile technologies 1.3 compare the relative severity of mobile security issues 1.4 explain a secure application development process 1.5 summarise application security best practices 1.6 identify the major architectural risks of weaknesses in an application.

Learning outcome
The learner will: 2. Understand Objective-C coding.
Assessment criteria
The learner can: 2.1 explain factors that should be considered when designing apps using Objective-C language 2.2 manage sensitive data in memory 2.3 explain Objective-C framework paradigms 2.4 explain Objective-C framework security impacts 2.5 identify code that gives correct interaction with iOS security facilities and objects.

Learning outcome
The learner will: 3. Understand application security features.
Assessment criteria
The learner can: 3.1 summarise the security features of the platform 3.2 explain the data protection Application Programming Interface (API) 3.3 explain the features of the security framework 3.4 explain the security of the keychain 3.5 explain the limitations of the keychain 3.6 use keychain for storing sensitive data.

Learning outcome
The learner will: 4. Understand network security.
Assessment criteria
The learner can: 4.1 summarise the risks in performing Web and network communications 4.2 implement a Secure Socket Layer (SSL) session with validation 4.3 explain threats to Web services 4.4 distinguish security protections for authentication 4.5 describe proper implementation of session security.

Learning outcome
The learner will: 5. Understand data security.
Assessment criteria
The learner can: 5.1 explain a secure data storage and encryption implementation 5.2 describe implementation of encryption in iOS to ensure data security 5.3 describe Apple Data Encryption APIs 5.4 explain how data is deleted securely 5.5 explain data recovery techniques for iOS 5.6 explain types of data 5.7 explain sensitivity of data 5.8 explain how data can leak.

Learning outcome
The learner will: 6. Understand application hardening.
Assessment criteria
The learner can: 6.1 explain application object binaries 6.2 explain application tools 6.3 explain Objective-C debugging 6.4 describe forms of abusive runtime manipulation 6.5 summarise counter-runtime abuse techniques.

Unit 616 Developing security for mobile apps on android

UAN:	**T/507/0226**
Level:	3
Credit value:	13
GLH:	73
Aim:	This unit is for those with experience of app development and familiarity with Java, the Android SDK, and principles of secure application development. It will develop learners' knowledge of the fundamental principles of application security, the security model of Android devices, Web services security model and vulnerabilities and common implementations of cryptography. Learners will develop skills needed to develop moderately complex applications using the Android SDK, use the security features of the Android operating system and APIs, implement secure coding techniques and harden an application against attack to levels appropriate.

Learning outcome
The learner will: 1. Understand application security.
Assessment criteria
The learner can: 1.1 identify legislation for secure mobile development 1.2 compare the relative severity of security issues 1.3 explain a secure development process throughout application development 1.4 summarise application security best practices 1.5 identify the architectural risks to weaknesses in an application.

Learning outcome
The learner will: 2. Understand application security features.
Assessment criteria
The learner can: 2.1 summarise the Android security architecture 2.2 explain the Android permission model 2.3 describe secure inter-process communication 2.4 securely implement common features.

Learning outcome
The learner will: 3. Understand network security.
Assessment criteria
The learner can: 3.1 summarise the risks in performing web and network communications 3.2 implement a Secure Socket Layer (SSL) session with validation 3.3 explain threats to web services 3.4 explain protections to web services 3.5 distinguish security protections for authentication 3.6 describe proper implementation of session security.

Learning outcome
The learner will: 4. Understand data security.
Assessment criteria
The learner can: 4.1 explain how encryption works 4.2 explain how hashing works 4.3 summarise methods for securing stored data 4.4 distinguish implementation of encryption in an Android application 4.5 implement data security using the Android permissions model 4.6 explain reverse engineering 4.7 explain reverse engineering countermeasures.

Learning outcome
The learner will: 5. Understand secure Java coding.
Assessment criteria
The learner can: 5.1 explain Java language structure 5.2 explain object-oriented development 5.3 use techniques for dealing with sensitive information 5.4 explain secure Java coding best practices.

Unit 617 Fundamentals of Windows based server administration

UAN:	**R/507/0234**
Level:	2
Credit value:	10
GLH:	55
Aim:	This unit provides the underpinning knowledge to install, configure and administer a Windows server. It offers learning about specific aspects of a server including the role of a Server, use of Active Directories, server performance management and server storage. The learner will also have an opportunity to demonstrate application of the knowledge.

Learning outcome
The learner will: 1. Know the fundamentals of a server.
Assessment criteria
The learner can: 1.1 describe how **device drivers are managed** 1.2 describe how **services are managed** 1.3 identify **server installation options**.

Range
device drivers are managed (installation, removal, disabling, update/upgrade, rollback, troubleshooting, Plug and Play, driver signing) **services are managed** (service status, startup types, recovery options, service accounts, dependencies) **server installation options** (correct version, partitioning, interactive install, unattended install, automated install, upgrade, firmware updates, minimal vs full)

Learning outcome
The learner will: 2. Know the roles of a server.
Assessment criteria
The learner can: 2.1 identify **application servers** 2.2 describe **web services** 2.3 describe **remote access services** 2.4 describe **file services** 2.5 describe **print services** 2.6 describe **server virtualisation**.

Range
application servers (mail, database, collaboration, monitoring, threat management) **web services** (WWW, FTP, adding components, sites, ports, SSL, certificates), **remote access services** (remote assistance, remote administration tools, remote desktop services, licensing, Virtual Private Network, multiple ports) **file services** (permissions, rights, auditing, sharing) **print services** (local printers, network printers, printer pools, Web printing, driver deployment, print job management) **server virtualisation** (virtualisation modes, virtual hard drives, virtual memory, virtual networks, checkpoints, physical to virtual, virtual to physical)

Learning outcome
The learner will: 3. Know types of server storage.
Assessment criteria
The learner can: 3.1 identify **storage technologies** 3.2 describe advantages and disadvantages of storage technologies 3.3 identify **RAID** 3.4 describe **disk types**.

Range
storage technologies (local (SATA, SCSI, IDE), NAS, SAN, fibre channel, iSCSI, NFS) **RAID** (types, combinations, hardware, software) **disk types** (basic, dynamic, mount points, file systems, VHD, distributed file systems)

Learning outcome
The learner will: 4. Know what active directory does.
Assessment criteria
The learner can: 4.1 describe **user accounts** 4.2 describe **groups** 4.3 describe **organisational units** 4.4 describe **containers** 4.5 describe **directory infrastructure** 4.6 describe **group policy**.

Range
user accounts (domain, local, profiles) **groups** (types, scopes, nesting) **organisational units** (purpose, delegation) **containers** (purpose, delegation) **directory infrastructure** (domain controllers, forests, roles, domains, trusts, functional levels, namespace, sites, replication) **group policy** (processing, management, computer policies, user policies, local policies)

Learning outcome
The learner will: 5. Know what is involved in server performance management.
Assessment criteria
The learner can: 5.1 identify **server hardware components** 5.2 describe how to **monitor** server performance.

Range
server hardware components (memory, disk, processor, network, removable drives, graphic cards, cooling, power usage, ports) **monitor** (methodology, procedures, tools, logs, alerts)

Learning outcome
The learner will: 6. Know what is involved in sever maintenance.
Assessment criteria
The learner can: 6.1 describe the start-up process 6.2 describe how **business continuity is maintained** 6.3 identify **updates** required to maintain server integrity 6.4 describe troubleshooting methodology.

Range
business continuity is maintained (backup and restore, disaster recovery, clustering, data redundancy, UPS) **updates** (software, driver, operating systems, service packs, critical, security, definitions, update services)

Learning outcome
The learner will: 7. Be able to administer windows-based servers.
Assessment criteria
The learner can: 7.1 configure a windows-based server 7.2 configure **storage** 7.3 configure **active directory** 7.4 troubleshoot a windows-based **server**.

Range
server (configure also means install) (install, upgrade ADDS, DNS, DHCP) **storage** (network drives, RAID, VHDs) **active directory** (users, groups, organisational units, group policy) **server** (performance, access issues, services)

Unit 618 Fundamentals of database administration

UAN:	**M/507/0774**
Level:	2
Credit value:	8
GLH:	40
Aim:	This unit covers concepts and technologies pertaining to Database Administration. Learners will gain knowledge about relational databases, queries, stored procedures, and the security requirement for databases and the data stored in them. And be able to show some of those skills in practice.

Learning outcome
The learner will: 1. Know core database concepts.
Assessment criteria
The learner can: 1.1 describe the **structure of a database** 1.2 describe relational database concepts 1.3 describe **Data Manipulation Language (DML)** 1.4 define Data Definition Language (DDL) 1.5 describe how T-SQL can be used to create database objects.

Range
structure of a database (tables, columns, rows, fields, records) **database concepts** (purpose, needs, management) **Data Manipulation Language (DML)** (definition, role)

Learning outcome
The learner will: 2. Know how to create database objects.
Assessment criteria
The learner can: 2.1 Select data types 2.2 Identify SQL syntax required to create tables in a database 2.3 Describe how to create views 2.4 Describe how to create stored **functions**.

Range
functions (select, insert, update, delete)

Learning outcome
The learner will: 3. Know how to manipulate data.
Assessment criteria
The learner can: 3.1 describe how to **select data** 3.2 describe how to use INSERT queries 3.3 describe how to **update data** 3.4 describe how to **delete data.**

Range
select data (use SELECT queries, use joins, combine results) **update data** (use UPDATE statements, using a table) **delete data** (from single and multiple tables, maintain data and referential integrity)

Learning outcome
The learner will: 4. Know how data is stored in a database.
Assessment criteria
The learner can: 4.1 describe levels of normalisation 4.2 describe how to normalise a database to third normal form 4.3 describe the reason for keys in a database 4.4 select primary keys 4.5 select data type for keys 4.6 select fields for composite keys 4.7 describe the relationship between foreign and primary keys 4.8 describe the purpose of **indexes** in a database.

Range
indexes (clustered, non-clustered)

Learning outcome
The learner will: 5. Know database administration.
Assessment criteria
The learner can: 5.1 Describe the importance of database security 5.2 Identify database objects that can be secured 5.3 Identify database objects that should be secured 5.4 Describe the roles of user accounts 5.5 Describe types of **database backup** 5.6 Describe how to restore a database.

Range
database backup (full, incremental, differential, partial)

Learning outcome
The learner will: 6. Be able to create and configure a database.
Assessment criteria
The learner can: 6.1 create **database objects** 6.2 manipulate **data** 6.3 configure **database** 6.4 implement **database security**.

Range
database objects (data types, tables, views, stored functions) **data** (SELECT, INSERT, UPDATE, DELETE) **database** (normalise, primary keys, foreign keys, clustered indexes) **database security** (authentication, backup)

Unit 619 Fundamentals of Windows based operating systems

UAN:	**A/507/0776**
Level:	2
Credit value:	8
GLH:	42
Aim:	This unit has been designed to help a learner build an understanding of these topics: Operating System Configurations, Installing and Upgrading Client Systems, Managing Applications, Managing Files and Folders, Managing Devices, and Operating System Maintenance. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • understand operating system configurations • install and upgrade client systems • manage applications • manage files and folders • manage devices • understand operating system maintenance.

Learning outcome
The learner will: 1. Know operating system configurations.
Assessment criteria
The learner can: 1.1 describe **control panel** configuration options 1.2 describe how to configure **desktop settings** 1.3 describe the function of native applications guidance whichever is built in 1.4 describe the function of **native tools.**

Range
control panel (administrative tools, accessibility options) **desktop settings** (profiles, display settings, shortcuts) **native tools** (configuration, mobility, remote management and assistance)

Learning outcome
The learner will: 2. Know the requirements for installing client systems.
Assessment criteria
The learner can:

2.1 identify operating system edition requirements 2.2 identify upgrade paths 2.3 identify application compatibility 2.4 understand installation **types** 2.5 identify requirements for virtualized clients.

Range
types (removable media, network, cloud)

Learning outcome
The learner will: 3. Know how to manage applications.
Assessment criteria
The learner can: 3.1 describe application **installations** 3.2 identify user account control **settings** 3.3 describe how to remove malicious software 3.4 describe how **services are managed** 3.5 describe application virtualization.

Range
installations (local, network, application removal) **settings** (standard user, administrative user, prompts, levels) **services are managed** (service status, startup types, recovery options, service accounts, dependencies)

Learning outcome
The learner will: 4. Know how to manage file systems.
Assessment criteria
The learner can: 4.1 describe file systems 4.2 describe **file sharing** 4.3 describe print sharing 4.4 describe **encryption options** 4.5 describe how to **configure libraries**.

Range
file sharing (security permissions, share permissions, effective permissions, mapping drives) **encryption options** (full disk encryption, encrypting file systems) **configure libraries** (offline files, multiple local locations, network locations).

Learning outcome
The learner will: 5. Know how to manage devices.
Assessment criteria
The learner can: 5.1 describe how to **connect devices** 5.2 describe **types of storage** 5.3 describe **printing options** 5.4 describe **system devices.**

Range
connect devices (plug and play, printers, third party software) **types of storage** (disk types, device types, drive types, cloud storage, security) **printing options** (local printers, network printers, print queues, print-to-file, Internet printing) **system devices** (video, audio, input, device management)

Learning outcome
The learner will: 6. Know operating system maintenance.
Assessment criteria
The learner can: 6.1 describe backup and recovery methods 6.2 describe native maintenance tools 6.3 identify **updates** required to maintain operating system integrity.

Range
updates (software, driver, operating systems, service packs, critical, security, definitions, hotfixes)

Learning outcome
The learner will: 7. Be able to configure Windows based operating systems.
Assessment criteria
The learner can: 7.1 **configure** a Windows based Operating System (OS) 7.2 manage applications 7.3 **customise** a Windows based operating system to meet requirements 7.4 **configure file** systems 7.5 manage devices 7.6 **maintain** a Windows based **operating system**.

Range
configure Operating System (OS) (installation, upgrade) **customise** Operating System (OS) (desktop, taskbar, start menu, networking) **configure file** system (compression, encryption, libraries) **maintain** Operating System OS (backup, restore)

Unit 620 Software development fundamentals

UAN:	**H/507/0271**
Level:	2
Credit value:	10
GLH:	61
Aim:	This unit has been designed to help a learner build an understanding of these topics: Core Programming, Object-Oriented Programming, General Software Development, Web Applications, Desktop Applications, and Databases. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • understand core programming • understand object-oriented programming • understand general software development • understand web applications • understand desktop applications • understand databases.

Learning outcome
The learner will: 1. Know the fundamentals of core programming.
Assessment criteria
The learner can: 1.1 describe how information is stored in computer memory 1.2 describe memory size requirements for data storage types 1.3 describe computer **decision structures** 1.4 identify **methods for handling repetition** 1.5 describe how errors are handled.

Range
decision structures (IF, multiple, decision tables, evaluating expressions, flowcharts) **methods for handling repetition** (For loops, While loops, Do. While loops, recursion)

Learning outcome
The learner will: 2. Know what is involved in object-orientated programming.
Assessment criteria
The learner can: 2.1 describe the **fundamentals of classes** 2.2 describe how to create a class 2.3 describe how to use classes in code 2.4 describe the concepts of object-oriented programming (inheritance, polymorphism, encapsulation).

Range
fundamentals of classes (properties, methods, events, constructors)

Learning outcome
The learner will: 3. Know requirements for software development.
Assessment criteria
The learner can: 3.1 describe phases of application lifecycle management 3.2 interpret application specifications 3.3 identify algorithms (arrays, stacks, queues, linked lists, sorting) 3.4 describe performance implications of data structures 3.5 select a data structure to meet requirements.

Learning outcome
The learner will: 4. Know requirements for web application development.
Assessment criteria
The learner can: 4.1 identify functions of **web technologies** 4.2 describe **web application development** 4.3 describe how to **host webpages** 4.4 describe how to access web services from client applications 4.5 describe the implementation of Web services (SOAP, Web Service Definition Language (WSDL)).

Range
web technologies (HTML, CSS, JavaScript) **web application development** (page life cycle, event model, state management, client-side vs server-side programming) **host webpages** (virtual directories, Web server)

Learning outcome
The learner will: 5. Know the requirements to create desktop applications.
Assessment criteria
The learner can: 5.1 describe how to create desktop applications (SDI, MDI, UI design, visual inheritance) 5.2 describe **console-based applications** 5.3 describe **windows-based system services**.

Range
console based applications (capabilities, characteristics) **windows based system services** (capabilities, characteristics)

Learning outcome
The learner will: 6. Know how to store and use data.
Assessment criteria
The learner can: 6.1 describe **relational database management systems** 6.2 describe database **query methods** 6.3 describe methods to connect to **data stores**.

Range
relational database management systems (capabilities, characteristics, design, ERDs, normalisation) **query methods** (SQL, creating and accessing stored procedures) **data stores** (flat file, XML, in-memory object)

Learning outcome
The learner will: 7. Be able to create applications and store data.
Assessment criteria
The learner can: 7.1 create a program 7.2 create an object-oriented program 7.3 create a web-based application 7.4 create a desktop-based application 7.5 create a database.

Unit 621 Gaming development fundamentals

UAN:	**K/507/0272**
Level:	2
Credit value:	8
GLH:	45
Aim:	This unit has been designed to help a learner build an understanding of these topics: Game Design, Hardware, Graphics, and Animation. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • understand game design • understand hardware • understand graphics • understand animation.

Learning outcome
The learner will: 1. Know key aspects of game design.
Assessment criteria
The learner can: 1.1 compare game **platforms** 1.2 compare game **genres** 1.3 describe how **game design** motivates the player 1.4 describe game **user interface** 1.5 describe artificial intelligence (AI) 1.6 differentiate between tool creation and game programming 1.7 describe how to **capture user data** 1.8 describe the architecture of an XNA game 1.9 describe **XNA hierarchy**.

Range
platforms (console, mobile, PC) **genres** (MMORPG, fantasy, sports, role playing, card, board, action) **game design** (quests, tasks, activities, how to win, game goals) **user interface** (UI layout and concepts, asset management, game state, gamer services) **capture user data** (save and restore user data, save and restore game state, handle input states, store data, manage game state) **XNA hierarchy** (initialisation, update loop, drawing)

Learning outcome
The learner will: 2. Know types of gaming hardware and their management.
Assessment criteria
The learner can: 2.1 select an **input device** 2.2 select an **output device** 2.3 describe how to **configure games in a network** 2.4 describe how to **manage game performance**.

Range
input device (mouse, keyboard, motion sensing, console, mobile) **output device** (screen, television, hand-held, local speakers, surround sound) **configure games in a network** (setting up Web services, TCP, UDP, basic management, no network access) **manage game performance** (CPUvs GPU, reach vs HiDef)

Learning outcome
The learner will: 3. Know how to create gaming graphics.
Assessment criteria
The learner can: 3.1 describe **rendering engines** 3.2 plan for **game state** 3.3 describe how to draw **objects.**

Range
rendering engines (DirectX, video and audio compression, resolution) **game state** (scene hierarchy engine, gametime to handle frame rate variations, games' main loop, graphics pipeline, game flow, loading, menus, save-load, configuration) **objects** (sprites, bitmaps, vector graphics, lighting, blending, text, textures, 3D geometry, parallax mapping, shaders, sprite font)

Learning outcome
The learner will: 4. Know how to implement gaming animation.
Assessment criteria
The learner can: 4.1 describe how to **animate** characters 4.2 describe how to **transform** objects 4.3 describe how to **manage collisions**.

Range
animate (movement, lighting, projections, shading, textures, sprite) **transform** forming, deforming, moving, point distances, planes, interpolation, scale, rotation) **manage collisions** (per pixel and rectangle collisions, collision detection, collision response, fundamentals of physics simulation)

Learning outcome
The learner will: 5. Be able to create games.
Assessment criteria
The learner can: 5.1 design game mechanics 5.2 design game dynamics 5.3 create a game user interface 5.4 create gaming animation.

Unit 622 HTML5 application development fundamentals

UAN:	**M/507/0273**
Level:	2
Credit value:	8
GLH:	41
Aim:	This unit has been designed to help a learner build an understanding of these topics: Manage the Application Life Cycle, Build the User Interface by Using HTML5, Format the User Interface by Using CSS, Code by Using JavaScript. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • manage the Application Life Cycle • build the User Interface by Using HTML5 • format the user interface by using CSS • code by Using JavaScript.

Learning outcome
The learner will: 1. Know how to manage the application life cycle.
Assessment criteria
The learner can: 1.1 describe **platform fundamentals** 1.2 describe how to manage the **state** of an application 1.3 describe how to debug a HTML5 touch enabled application 1.4 describe how to test a HTML5 touch enabled application 1.5 describe how to publish an application to a store.

Range
platform fundamentals (packaging and the runtime environment) **state** (session state, app state, persist state)

Learning outcome
The learner will: 2. Know how to build the user interface using HTML5.
Assessment criteria
The learner can: 2.1 identify HTML5 tags to display text content 2.2 identify HTML5 **tags to display graphics** 2.3 identify HTML5 tags to play **media** 2.4 identify HTML5 tags to **organise content** 2.5 identify HTML5 tags to organise forms 2.6 Identify HTML5 tags for input 2.7 Identify HTML5 tags for validation.

Range
tags to display graphics (Canvas, SVG) **media** (video, audio) **organise content** (tables, lists, sections)

Learning outcome
The learner will: 3. Know how to format the user interface using CSS.
Assessment criteria
The learner can: 3.1 describe core **CSS concepts** 3.2 describe how to **arrange user interface (UI) content** using CSS 3.3 describe how to **manage the flow of text** content using CSS 3.4 describe how to create **graphic effects** using CSS.

Range
CSS concepts (separate presentation from content, manage content flow, manage positioning of individual elements, basic CSS styling) **arrange user interface (UI) content** (flexible box, grid layouts, proportional scaling, templates) **manage the flow of text** (regions, columns, hyphenation, positioned floats) **graphic effects** (rounded corners, shadows, transparency, background gradients, typographic, 2D and 3D transformations)

Learning outcome
The learner will: 4. Know how to code using JavaScript.
Assessment criteria
The learner can: 4.1 describe how to **manage Java Script** 4.2 describe how to **update the UI** using JavaScript 4.3 identify JavaScript animation code 4.4 describe **how to access data** using JavaScript 4.5 identify code that responds to touch 4.6 identify HTML5 **API** code 4.7 describe how to access **system resources**.

Range
manage Java script (use of functions, use of libraries) **update the UI** (locating elements, responding to events, showing and hiding elements, updating content of elements, adding elements) **how to access data** (send and receive data, transmit complex objects, parsing, accessing databases and indexed DB, loading and saving files, App Cache) **API** (GeoLocation, Web Workers, Web Sockets) **system Resources** (operating systems, system devices)

Learning outcome
The learner will: 5. Be able to create HTML5 based web applications.
Assessment criteria
The learner can: 5.1 build user interface using HTML5 5.2 format user interface using CSS 5.3 access data using JavaScript.

Unit 623 Software testing fundamentals

UAN:	**H/507/0285**
Level:	2
Credit value:	8
GLH:	39
Aim:	This unit has been designed to help a learner build an understanding of these topics: test methodologies. It also focuses on working with software bugs, creating and managing software tests, and even test automation. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • understand test methodologies • understand how to manage software bugs • understand how to create and manage software tests • understand the basics of test automation.

Learning outcome
The learner will: 1. Know what the testing fundamentals are.
Assessment criteria
The learner can: 1.1 describe **software testing** 1.2 describe **system components** 1.3 describe **fundamentals of programming** 1.4 describe application **lifecycle** management.

Range
software testing (measuring software quality, testing benefits) **system components** (hardware, software, network, interaction and dependencies) **fundamentals of programming** (data types, programming languages, algorithms) **lifecycle** (agile, waterfall, spiral)

Learning outcome
The learner will: 2. Know what is meant by testing methodology.
Assessment criteria
The learner can: 2.1 describe **testing techniques** 2.2 describe **testing levels** 2.3 describe **testing types**.

Range
testing techniques (manual, automated, white box, black box) **testing levels** (unit, component, integration) **testing types** (functional, performance structural, regression, security, stress, accessibility, usability, localisation)

Learning outcome
The learner will: 3. Know how to create software tests.
Assessment criteria
The learner can: 3.1 describe **user-centric testing** 3.2 describe **software testability** 3.3 describe **test plan components** 3.4 describe **feature tests** 3.5 define **scope of test cases**.

Range
user-centric testing (business needs and issues, customer requirements, scenarios) **software testability** (test driven development, testing hooks) **test plan components** (test schedule, scope, methodology, scenarios, tools) **feature tests** (boundary conditions, level of details, validity) **scope of test cases** (boundary conditions, level of details, validity)

Learning outcome
The learner will: 4. Know how to manage software testing projects.
Assessment criteria
The learner can: 4.1 describe **testing milestones** 4.2 describe the **agile process** 4.3 describe how to **work with distributed teams** 4.4 define **test reports**.

Range
testing milestones (process fundamentals, exit criteria, sign off) **agile process** (scrum, Kanban, sprint management) **work with distributed teams** (communication, risk management, schedule management, delivery process) **test reports** (communication, risk management, schedule management, delivery process)

Learning outcome
The learner will: 5. Know how to manage bugs.
Assessment criteria
The learner can: 5.1 describe how to detect software defects 5.2 describe how to **log bugs** 5.3 describe how to **manage bugs.**

Range
log bugs (priority, severity, dependency, reproducing steps) **manage bugs** (triage, resolution, closing, monitoring, reporting)

Learning outcome
The learner will: 6. Know how to automate software testing.
Assessment criteria
The learner can: 6.1 describe **test automation** 6.2 define test **automation strategies** 6.3 describe how to **write automated tests** 6.4 describe how to **manage test scripts**.

Range
test automation (benefits, process, suitability) **automation strategies** (code coverage, logging, automation priority) **write automated tests** (logic, error handling, commenting, virtual machines) **manage test scripts** (build verification test, lab management)

Learning outcome
The learner will: 7. Be able to test software.
Assessment criteria
The learner can: 7.1 create software tests 7.2 manage software testing projects 7.3 manage bugs 7.4 automate software testing.

Unit 624 Networking fundamentals

UAN:	**Y/507/0283**
Level:	2
Credit value:	9
GLH:	47
Aim:	This unit has been designed to help a learner build an understanding of these topics: Network Infrastructures, Network Hardware, and Protocols and Services. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • understand network infrastructures • understand network hardware • understand protocols and services.

Learning outcome
The learner will: 1. Know key aspects of network infrastructures.
Assessment criteria
The learner can: 1.1 describe differences between the Internet, intranet and extranet 1.2 describe **Local Area Networks (LANs)** 1.3 describe **Wide Area Networks (WANs)** 1.4 describe **wireless networking** 1.5 describe **wireless security** 1.6 describe **network topologies**.

Range
Local Area Networks (LANS) (perimeter networks, addressing, VLANs, wired, wireless) **Wide Area Networks (WANS)** (types, characteristics) **wireless networking** (types, characteristics) **wireless security** (keys, SSID, MAC filters) **network topologies** (star, mesh, ring, access methods)

Learning outcome
The learner will: 2. Know network hardware.
Assessment criteria
The learner can: 2.1 describe how **switches function** 2.2 describe how **routers function** 2.3 describe **media types** 2.4 describe **media type characteristics** 2.5 explain **factors** affecting media types.

Range
switches function (number and type of ports, number of uplinks, managed, unmanaged, VLAN capabilities, Layer 2, Layer 3, security options, hardware redundancy, switching types, MAC table, hubs vs switches) **routers function** (directly connected routes, static routing, dynamic routing, default routes, routing table, NAT, transmission speeds, software routing) **media types** (fibre optic, UTP, STP, wireless) **media type characteristics** (media segment length and speed) **factors** (external interference, electricity, interception)

Learning outcome
The learner will: 3. Know networking protocols.
Assessment criteria
The learner can: 3.1 describe the OSI model guidance, what happens at each layer and how it supports the relationship between protocols and services 3.2 describe **IPv4** 3.3 describe **IPv6** 3.4 describe how to use **TCP/IP** tools.

Range
IPv4 (addressing, subnetting, NAT, static IP, gateway, APIPA, network classes) **IPv6** (addressing, tunneling, dual ip stack, subnetmask, gateway, packets) **TCP/IP tools** (ping, tracert, pathping, Telnet, IPconfig, netstat)

Learning outcome
The learner will: 4. Know networking services.
Assessment criteria
The learner can: 4.1 describe names resolution process 4.2 describe **networking services**.

Range
networking services (DHCP, IPsec, remote access)

Learning outcome
The learner will: 5. Be able to set up networks.
Assessment criteria
The learner can: 5.1 set up a **network** 5.2 configure **network hardware** 5.3 configure network protocols 5.4 troubleshoot networking.

Range
network (LAN, wireless) **network hardware** (switches, routers, network media)

Unit 625 IT security fundamentals

UAN:	**J/507/0277**
Level:	2
Credit value:	8
GLH:	43
Aim:	This unit has been designed to help a learner build an understanding of these topics: Security Layers, Operating System Security, Network Security, Security Software. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • understand security layers • understand operating system security • understand network security • understand security software.

Learning outcome
The learner will: 1. Know key aspects of security layers.
Assessment criteria
The learner can: 1.1 describe **core security principles** 1.2 describe how threat and risk impact upon core security principles 1.3 describe **physical security** 1.4 describe **Internet security** 1.5 describe **types of wireless security** 1.6 describe advantages and disadvantages of **types of wireless security.**

Range
core security principles (confidentiality, integrity, availability, least privilege, social engineering, attack surface,) **physical security** (site security, computer security, removable devices and drives, mobile device security) **internet security** (browser settings, zones, secure Web sites) **types of wireless security** (keys, SSID, MAC filters)

Learning outcome
The learner will: 2. Know requirements and issues of operating system security.
Assessment criteria
The learner can: 2.1 describe **user authentication** 2.2 describe how to configure **permissions** 2.3 describe password policies 2.4 describe audit policies 2.5 describe **encryption options** 2.6 describe **types of malware.**

Range
user authentication (multifactor, smart cards, remote authentication, PKI, certificates, biometrics, time skew, password reset, administrative privileges) **permissions** (security, share, inheritance, effective, basic, advanced, taking ownership, delegation) **encryption options** (EFS, full disk encryption, PKI, VPN, certificates, algorithms, public/private keys, encryption software, token devices) **types of malware** (buffer, overflow, worms, Trojans, spyware, viruses, keyloggers)

Learning outcome
The learner will: 3. Know requirements to establish network security.
Assessment criteria
The learner can: 3.1 describe **types of firewall** 3.2 describe **network access protection** 3.3 describe **network isolation** 3.4 describe how to maintain **protocol security.**

Range
types of firewall (hardware, software, stateful, stateless, secure content management, unified threat management) **network access protection** (purpose, requirements) **network isolation** (VLANs, routing, honeypot, NAT, perimeter network, VPN, IPsec, server and domain isolation) **protocol security** (spoofing, IPsec, tunnelling, sniffing, DNSsec, common attack methods)

Learning outcome
The learner will: 4. Know protection options of system security.
Assessment criteria
The learner can: 4.1 describe **client protection options** 4.2 describe **email protection options** 4.3 describe **server protection options.**

Range
client protection options (anti-virus, built-in settings, updates, encrypting offline folders, application restrictions) **email protection options** (anti-spam, anti-virus, spoofing, phishing, pharming, client vs server protection, sender policy framework, PTR records) **server protection options** (separation of services, hardening, updates, disabling unsecure protocols, security analysis software)

Learning outcome
The learner will: 5. Be able to configure security for IT systems.
Assessment criteria
The learner can: 5.1 configure operating system security 5.2 configure network security 5.3 configure service security.

Unit 626 Windows development fundamentals

UAN:	**M/507/0287**
Level:	2
Credit value:	8
GLH:	38
Aim:	This unit has been designed to help a learner build an understanding of these topics: Windows Programming Basics, Creating Windows Forms Applications, Creating Windows Services Applications, Accessing Data in a Windows Forms Application, and Deploying a Windows Application. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • understand Windows programming basics • create Windows services applications • create Windows services applications • access data in a Windows forms application • deploy a Windows application.

Learning outcome
The learner will: 1. Know how to create Windows applications.
Assessment criteria
The learner can: 1.1 identify types of Windows applications 1.2 describe user interface (UI) design principles 1.3 describe how to create Windows-based applications.

Learning outcome
The learner will: 2. Know how to create Windows Form applications.
Assessment criteria
The learner can: 2.1 describe how to **manage events** 2.2 describe forms inheritance in applications 2.3 describe how to **manage controls** 2.4 describe how to implement user input 2.5 describe how to validate user input 2.6 identify issues in code 2.7 describe how to debug a Windows based application.

Range
manage events (creating events, handling events) **manage controls** (create new controls, extend controls)

Learning outcome
The learner will: 3. Know how to create Windows Services applications.
Assessment criteria
The learner can: 3.1 describe how to create a Windows Services application 3.2 describe how to create installers for Windows Services application.

Learning outcome
The learner will: 4. Know how to access data in Windows form applications.
Assessment criteria
The learner can: 4.1 describe how to connect a Windows based application to a database 4.2 describe **databound controls.**

Range
databound controls (how data is bound to controls, how to display data, validating databound items)

Learning outcome
The learner will: 5. Know how to deploy Windows applications.
Assessment criteria
The learner can: 5.1 describe methods of deploying Windows applications 5.2 select a method for deploying Windows applications 5.3 describe how to create **setup projects** for applications.

Range
Setup projects (specify custom actions, create special folders, security requirements, program file location)

Learning outcome
The learner will: 6. Be able to create Windows applications.
Assessment criteria
The learner can: 6.1 design a user interface 6.2 create a Windows Form application 6.3 create a Windows Services application 6.4 create an Installer for a Windows application 6.5 connect a Windows application to a database 6.6 create a Setup project for an application.

Unit 627 Web development fundamentals

UAN:	**K/507/0286**
Level:	2
Credit value:	8
GLH:	43
Aim:	This unit has been designed to help a learner build an understanding of these topics: Programming Web Applications, Working with Data and Services, Troubleshooting and Debugging Web Applications, Working with Client-Side Scripting, and Configuring and Deploying Web Applications. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • program web applications • work with data and services • troubleshoot and debug web applications • work with client-side scripting • configure and deploy web applications.

Learning outcome
The learner will: 1. Know how to programme web applications.
Assessment criteria
The learner can: 1.1 describe how to **customise** web pages 1.2 describe intrinsic objects 1.3 describe different **types of state** 1.4 describe how state is stored 1.5 describe how **events** control page flows 1.6 describe **controls** required for a scenario 1.7 describe configuration files.

Range
customise (layout, appearance, HTML, CSS, embedding images, navigation, tables) **types of state** (session state, view state, control state, application state) **events** (application and page life cycle events, page events, control events, application events, session events, cross-page posting) **control** (user, server, Web, validation)

Learning outcome
The learner will: 2. Know how to use data for webpages.

Assessment criteria
The learner can: 2.1 read XML data 2.2 write XML data 2.3 select a data object to meet requirements 2.4 describe how to call a service from a Web page 2.5 describe **datasource controls** 2.6 describe binding controls 2.7 describe how to manage data connections.

Range
datasource controls (LinqDataSource, ObjectDataSource, XmlDataSource, SqlDataSource)

Learning outcome
The learner will: 3. Know how to troubleshoot web applications.
Assessment criteria
The learner can: 3.1 describe how to **debug a web application** 3.2 describe how to troubleshoot http web application errors.

Range
debug a web application (custom error pages, error information, tracing)

Learning outcome
The learner will: 4. Know client-side scripting code and its purpose.
Assessment criteria
The learner can: 4.1 describe the purpose of client-side scripting 4.2 identify client-side scripting code 4.3 describe **AJAX concepts**.

Range
AJAX concepts (ASP.NET AJAX implementation, working with client-side libraries, EnablePartialRendering, Triggers, ChildrenAsTriggers, Scripts, Services, UpdateProgress, Timer, ScriptManagerProxy, extender controls)

Learning outcome
The learner will: 5. Know how to configure web applications.
Assessment criteria
The learner can: 5.1 describe how to **configure secure access** 5.2 describe how to configure **reference assemblies** 5.3 describe how to publish web applications 5.4 describe **application pools.**

Range
configure secure access (authentication, authorization, impersonation) **reference assemblies** (local assemblies, shared assemblies, for project, for solutions) **application pools** (purpose, effects on Web applications)

Learning outcome
The learner will: 6. Be able to create a web-based application.
Assessment criteria
The learner can: 6.1 program a **web application** 6.2 use events to control page flows 6.3 connect a web application to a database 6.4 troubleshoot a web application 6.5 configure a web application.

Range
web application (layout, appearance, HTML, CSS, embedding images, navigation, tables)

Unit 628 .NET fundamentals

UAN:	**F/507/0276**
Level:	2
Credit value:	9
GLH:	49
Aim:	This unit has been designed to help a learner build an understanding of these topics: .NET Framework Concepts, Namespaces and Classes in the .NET Framework, .NET Code Compilation, I/O Classes in the .NET Framework, Security, .NET Languages, and Memory Management. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to understand: • .NET framework concepts • namespaces and classes in the .NET Framework • NET code compilation • I/O Classes in the .NET Framework • security • .NET Languages • memory management.

Learning outcome
The learner will: 1. Know .NET framework concepts.
Assessment criteria
The learner can: 1.1 describe application settings 1.2 describe event handling in the **.NET** 1.3 describe structured **exception handling** in the .NET framework.

Range
NET framework (event-driven programming model, event handlers, raising events, implementing delegates) **exception handling** (error handling concepts, exceptions, exception types)

Learning outcome
The learner will: 2. Know key components in the .NET framework.
Assessment criteria
The learner can: 2.1 describe .NET class **hierarchies** 2.2 describe **object orientated concepts** in the .NET framework 2.3 describe .NET namespaces 2.4 describe **class libraries** 2.5 describe **data types** in the .NET framework 2.6 describe **generics**.

Range
hierarchies (system classes, classification of classes, logical organisation of classes) **object-orientated concepts** (inheritance, polymorphism, interfaces) **class libraries** (logical grouping of classes, logic of class libraries, importance of class libraries, purpose) **data types** (intrinsic data types, value types, reference types, boxing, unboxing, .NET collection classes) **generics** (infrastructure, interfaces, delegates, contravariant, covariant, methods, verifiability, constraints)

Learning outcome
The learner will: 3. Know the requirements of .NET code compilation.
Assessment criteria
The learner can: 3.1 describe how source code is compiled 3.2 describe strong naming 3.3 describe **version control** 3.4 describe **assemblies** 3.5 describe metadata.

Range
version control (how .NET applications are versioned, how to run different versions on the same computer) **assemblies** (.NET assemblies, shared assemblies)

Learning outcome
The learner will: 4. Know Input/Output (I/O) classes in the .NET framework.
Assessment criteria
The learner can: 4.1 describe .NET **file classes** 4.2 describe console I/O 4.3 describe **XML classes** in the .NET framework.

Range
file classes (read/write, stream readers and writers) **XML classes** (XMLReader, XMLWriter, SML Schemas)

Learning outcome
The learner will: 5. Know how to secure a .NET application.
Assessment criteria
The learner can: 5.1 describe **System Security namespace** 5.2 describe **code access security.**

Range
system security namespace (permissions, cryptography) **code access security** (authentication, authorisation, access control, policies)

Learning outcome
The learner will: 6. Know key aspects of .NET languages.
Assessment criteria
The learner can: 6.1 describe **language interoperability** 6.2 describe **type safety**.

Range
language interoperability (calling code in one language from another language, .NET language parity) **type safety** (memory type safety, type safety in classes, strong types, security policies)

Learning outcome
The learner will: 7. Know what is involved in memory management.
Assessment criteria
The learner can: 7.1 describe **resource allocation** 7.2 compare managed and unmanaged applications.

Range
Resource allocation (garbage collection, memory allocation, stack vs heap)

Learning outcome
The learner will: 8. Be able to create .NET applications.
Assessment criteria
The learner can: 8.1 create a class library in the .NET framework 8.2 compile a source code 8.3 secure a .NET application 8.4 create a .NET application.

Unit 629 Mobile development fundamentals

UAN:	**L/507/0281**
Level:	2
Credit value:	8
GLH:	41
Aim:	This unit has been designed to help a learner build an understanding of these topics: Work with Physical Devices, Use Data with Mobile Services, Use a Mobile Application Development Environment, Develop Mobile Applications. Learners are expected to be able to demonstrate this understanding, so that on successful completion of this unit they will be able to: • work with physical devices • use data with mobile services • use a mobile application development environment • develop mobile applications. This unit is linked to the Microsoft Official Academic Course (MOAC) Mobility and Device Fundamentals. .

Learning outcome
The learner will: 1. Understand mobile phone capabilities.
Assessment criteria
The learner can: 1.1 define phone **tools** 1.2 identify device sensors 1.3 describe Application Programming Interface (APIs) 1.4 identify built-in hardware 1.5 compare **devices** 1.6 identify ways to save energy.

Range
tools (development, testing, connecting) **devices** (features, API levels, number of touch points, networking capabilities)

Learning outcome
The learner will: 2. Understand the use of data with mobile devices.
Assessment criteria
The learner can: 2.1 describe how mobile devices integrate with databases 2.2 describe how to **minimise** data traffic 2.3 describe the benefits of database server replication 2.4 describe benefits of **data storage locations** 2.5 describe how to access native APIs 2.6 describe how to manage offline situations.

Range
minimise (for performance, for cost) **data storage locations** (local, isolated, remote)

Learning outcome
The learner will: 3. Understand the mobile application development environment.
Assessment criteria
The learner can: 3.1 describe mobile device design (concepts, globalisation, localisation, optimisation, architecture) 3.2 describe mobile **networking concepts** 3.3 evaluate development tools for mobile applications 3.4 describe how to create a deployment package 3.5 describe how to **debug mobile applications** 3.6 identify code errors 3.7 identify code to meet requirements 3.8 distinguish between programming languages.

Range
networking concepts (server/cloud communication, multicast, HTTP requests, use of web services, throttling, notifications, wireless network) **debug mobile applications** (create a test environment, test, debug)

Learning outcome
The learner will: 4. Understand how to develop mobile applications.
Assessment criteria
The learner can: 4.1 describe how to **manage** the application life cycle 4.2 describe mobile device **APIs** 4.3 explain the use of **mobile device controls** 4.4 describe how to **build** a User Interface (UI).

Range
Manage (preserving application state, tombstoning, balancing code, responsive applications, visible status, storing passwords) **API's** (navigation services, geolocation, Forms, Canvas and Media for HTML5, manipulation events) **mobile device controls** (native controls, custom controls, UI, notifications, to enhance application functionality) **build** (system theme, colour, orientation, graphic layering, integrating images and media, UI standards and guidelines

Learning outcome
The learner will: 5. Be able to create mobile applications.
Assessment criteria
The learner can: 5.1 create a mobile application 5.2 connect a mobile application to a database 5.3 create a deployment package 5.4 build a user interface.

Unit 630 Administering server databases

UAN:	**A/507/0292**
Level:	3
Credit value:	12
GLH:	48
Aim:	This unit is intended for those who are looking to become database professionals. A learner that achieves this unit will be able to perform installation, maintenance, and configuration tasks, as well as take responsibility for aspects of other activities such as setting up database systems, ensuring systems operate efficiently, and the regular storing, backing up, and securing data from unauthorised access. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam Administering Microsoft SQL Server Databases.

Learning outcome
The learner will: 1. Be able to install SQL Servers.
Assessment criteria
The learner can: 1.1 describe the SQL Server platform 1.2 use SQL Server tools 1.3 configure SQL Server services 1.4 describe the SQL Server architecture 1.5 plan for SQL Server resource requirements 1.6 conduct pre-installation stress testing for SQL Server 1.7 install SQL Server 1.8 upgrade SQL Server 1.9 automate the installation of SQL Server.

Learning outcome
The learner will: 2. Be able to use databases.
Assessment criteria
The learner can: 2.1 describe the role of SQL Server databases 2.2 describe the structure of SQL Server databases 2.3 administer files and filegroups 2.4 move database files 2.5 transfer data to and from SQL Server 2.6 optimise the bulk insert process.

Learning outcome
The learner will: 3. Be able to restore SLQ server databases.
Assessment criteria
The learner can: 3.1 describe the concepts of backup strategies 3.2 explain the transaction logging capabilities 3.3 plan a SQL Server backup strategy 3.4 manage database backups 3.5 describe the restore process 3.6 restore databases 3.7 use Point-in-time Recovery.

Learning outcome
The learner will: 4. Know how to authorise users.
Assessment criteria
The learner can: 4.1 describe how SQL Server authenticates connections 4.2 describe how logins are authorised to access databases 4.3 describe the requirements for authorisation across servers 4.4 authorise user access to objects 4.5 authorise users to execute code 4.6 configure permissions at the schema level 4.7 use **database server roles**.

Range
database server roles (fixed, user defined)

Learning outcome
The learner will: 5. Be able to audit SQL Server Environments.
Assessment criteria
The learner can: 5.1 describe the options for auditing data access in SQL Server 5.2 implement SQL Server Audit 5.3 manage SQL Server Audit.

Learning outcome
The learner will: 6. Be able to automate SQL Server Management.
Assessment criteria
The learner can: 6.1 automate SQL Server Management 6.2 use SQL Server Agent 6.3 manage SQL Server Agent jobs.

Learning outcome
The learner will: 7. Be able to configure security for SQL Server Agent.
Assessment criteria
The learner can: 7.1 explain SQL Server Agent security 7.2 configure credentials 7.3 configure Proxy accounts.

Learning outcome
The learner will: 8. Be able to perform ongoing database maintenance.
Assessment criteria
The learner can: 8.1 configure database mail 8.2 monitor SQL Server errors 8.3 configure operators 8.4 configure alerts 8.5 configure notifications 8.6 ensure database integrity 8.7 maintain indexes 8.8 automate routine database maintenance.

Learning outcome
The learner will: 9. Be able to use tracing options.
Assessment criteria
The learner can: 9.1 capture SQL Server activity 9.2 analyse performance data 9.3 improve SQL Server performance.

Learning outcome
The learner will: 10. Be able to manage multiple servers.
Assessment criteria
The learner can: 10.1 manage multiple servers 10.2 describe options for virtualising SQL Server 10.3 deploy Data-Tier Applications 10.4 upgrade Data-Tier Applications.

Learning outcome
The learner will: 11. Be able to troubleshoot SQL Server administrative issues.
Assessment criteria
The learner can: 11.1 explain SQL Server troubleshooting methodology 11.2 resolve administrative **issues**.

Range
issues (service-related, concurrency, login, connectivity)

Unit 631 Administering a Windows based server

UAN:	**A/507/0289**
Level:	3
Credit value:	11
GLH:	50
Aim:	This unit provides the skills and knowledge necessary to administer a Windows based Server. A learner achieving this unit will have the ability to administer the tasks required to maintain a Windows based Server infrastructure, such as user and group management, network access, and data security. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Administering Windows Server.

Learning outcome
The learner will: 1. Be able to deploy server images.
Assessment criteria
The learner can: 1.1 install Windows deployment services 1.2 describe how to create operating system images 1.3 configure **Windows deployment** services.

Range
Windows deployment (incorporates custom computer naming, deployment of images, administrative tasks)

Learning outcome
The learner will: 2. Be able to manage Domain Name Systems (DNS).
Assessment criteria
The learner can: 2.1 explain how to configure DNS zones and transfers 2.2 manage **DNS.**

Range
DNS (includes installing and configuring, troubleshooting server roles, zones, conditional forwarding, resource records)

Learning outcome
The learner will: 3. Be able to maintain domain controllers.
Assessment criteria
The learner can: 3.1 explain the structure of directory services 3.2 describe how to implement **domain controllers** 3.3 implement domain controllers 3.4 configure directory services snapshots 3.5 describe the use of domain controller cloning.

Range
domain controllers (virtualised, read only (RODCs)) **3.3** includes configuring, implementing, administering, troubleshoot DC includes virtualised, read only (RODCs)

Learning outcome
The learner will: 4. Be able to implement a group policy infrastructure.
Assessment criteria
The learner can: 4.1 configure managed **service accounts** 4.2 explain the features of group policy 4.3 implement group policy preferences 4.4 manage group policy scope 4.5 describe administrative templates 4.6 manage group **policy objects** 4.7 describe how to deploy software using group policy objects.

Range
service accounts (create, associate, password policy, account lockout) **policy objects** (create, configure, monitor, process policy, troubleshoot)

Learning outcome
The learner will: 5. Be able to manage remote access.
Assessment criteria
The learner can: 5.1 manage **remote access role** in Windows 5.2 manage an **advanced remote access infrastructure** 5.3 explain web application proxy (implementation, validation).

Range
remote access role (install, configure, monitor, troubleshoot) **advanced remote access infrastructure** (installation, configuring, monitoring, validate, including VPN)

Learning outcome
The learner will: 6. Be able to manage the network server.
Assessment criteria
The learner can: 6.1 describe network policy authentication methods 6.2 manage the **network policy server** 6.3 configure RADIUS clients 6.4 configure RADIUS servers 6.5 describe how network access protection can help protect a network 6.6 describe Network Access Protection enforcement processes 6.7 manage Network Access Protection.

Range
network policy server (configure troubleshoot) **network access protection** (configure troubleshoot)

Learning outcome
The learner will: 7. Be able to optimise file services
Assessment criteria
The learner can: 7.1 describe file server resource manager 7.2 configure file services 7.3 implement classification tasks 7.4 implement file management tasks 7.5 describe the components of the distributed file system 7.6 configure **distributed file systems** 7.7 encrypt files using encrypting file system EFS 7.8 configure advanced auditing features.

Range
distributed file systems (namespaces replication)

Learning outcome
The learner will: 8. Be able to manage group policy.
Assessment criteria
The learner can: 8.1 describe the role of Windows server update services 8.2 describe the use of monitoring tools for Windows Server 8.3 describe how to monitor events 8.4 establish a performance baseline 8.5 identify the source of a performance problem 8.6 configure centralised event logs 8.7 interpret events.

Unit 632 Configuring advanced Windows server services

UAN:	**R/507/0332**
Level:	3
Credit value:	12
GLH:	52
Aim:	This unit provides the skills and knowledge necessary to administer a Windows based server. A learner achieving this unit will have the ability to perform the advanced configuring tasks required to deploy, manage, and maintain a Windows Server Infrastructure, such as fault tolerance, certificate services, and identity federation. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Administering Windows Server.

Learning outcome
The learner will: 1. Be able to implement advanced network services.
Assessment criteria
The learner can: 1.1 configure advanced DNS services 1.2 configure advanced DHCP services 1.3 implement Internet Protocol Address Management (IPAM).

Learning outcome
The learner will: 2. Be able to implement advanced file services.
Assessment criteria
The learner can: 2.1 configure Internet Small Computer Storage Interface (ISCSI) storage 2.2 configure **BranchCache** 2.3 configure the File Classification Infrastructure 2.4 monitor BranchCache 2.5 optimise storage usage.

Range
BranchCache (Main Officer Servers, Branch Officer Servers, client computers)

Learning outcome
The learner will: 3. Be able to implement Dynamic Access control.
Assessment criteria
The learner can: 3.1 plan Dynamic Access control implementation 3.2 configure **claims** 3.3 configure resource property definitions 3.4 configure **central access** 3.5 validate dynamic access controls 3.6 remediate dynamic access controls 3.7 implement resource policies.

Range
claims (user device) **central access** (rules, policies)

Learning outcome
The learner will: 4. Be able to implement directory services.
Assessment criteria
The learner can: 4.1 describe distributed directory services deployments 4.2 implement a distributed directory services deployment 4.3 implement Child Domains 4.4 implement Forest Trusts 4.5 manage **directory services** 4.6 create subnets.

Range
directory services (create, configure, monitor, modify, troubleshoot, trusts, replication, sites (including default sites)

Learning outcome
The learner will: 5. Be able to implement certificate services.
Assessment criteria
The learner can: 5.1 configure certificates 5.2 configure key recovery 5.3 describe the Public Key Infrastructure (PKI) 5.4 deploy a certification authority 5.5 configure the certification authority hierarchy 5.6 manage certificates.

Range
5.1 includes templates enrolment revocation **5.6** deploy, implement distribution, implement revocation, recovery

Learning outcome
The learner will: 6. Be able to implement Rights Management Services (RMS).
Assessment criteria
The learner can: 6.1 describe RMS 6.2 configure RMS 6.3 implement RMS trust policies 6.4 verify RMS deployment 6.5 deploy RMS infrastructure 6.6 manage an RMS infrastructure 6.7 configure RMS content protection 6.8 configure external access to RMS.

Learning outcome
The learner will: 7. Be able to implement Federation Services (FS).
Assessment criteria
The learner can: 7.1 describe FS 7.2 configure FS pre-requisites 7.3 configure FS 7.4 deploy FS.

Range
7.3 and 7.4 for a single organisation, for Federated business partners

Learning outcome
The learner will: 8. Be able to implement Network Load Balancing (NLB).
Assessment criteria
The learner can: 8.1 manage an NLB cluster 8.2 validate high availability for an NLB cluster.

Range
8.1 Plan, Configure, Implement, monitor

Learning outcome
The learner will: 9. Be able to implement failover clustering.
Assessment criteria
The learner can: 9.1 manage a failover cluster 9.2 configure cluster-aware updating on a failover cluster 9.3 manage a highly available file server 9.4 configure a highly available failover solution 9.5 configuring a virtualised failover cluster for virtualisation 9.6 configure a Highly Available Virtual Machine 9.7 implement virtualisation of machines on failover clusters 9.8 implement virtual machine movement 9.9 manage virtual environments.

Range
9.1 includes implement, configure, maintain multi-site and single site **9.3** includes deploy, configure, validate **9.4** for services, for applications

Learning outcome
The learner will: 10. Be able to implement disaster recovery.
Assessment criteria
The learner can: 10.1 describe disaster recovery 10.2 implement server recovery 10.3 implement data recovery 10.4 back up data on a Windows server 10.5 use cloud services for disaster recovery.

Unit 633 Configuring Windows based systems

UAN:	**D/507/0334**
Level:	3
Credit value:	12
GLH:	52
Aim:	This unit provides the skills and knowledge necessary to configure or support Windows based systems. A learner achieving this unit will have the ability configure or support Windows computers, devices, users, and associated network and security resources. The networks will typically be configured as domain-based or peer-to-peer environments with access to the Internet and cloud services. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Configuring Windows.

Learning outcome
The learner will: 1. Be able to install Windows.
Assessment criteria
The learner can: 1.1 describe the different editions of Windows 1.2 describe options for upgrading a Windows based operating system 1.3 prepare a computer for Windows installation 1.4 install a Windows operating system 1.5 automate the installation of a Windows operating system 1.6 configure device drivers 1.7 explain Windows operating system licensing and activation 1.8 customise an image for deployment 1.9 prepare an image for deployment 1.10 describe volume activation 1.11 deploy a Windows Image.

Learning outcome
The learner will: 2. Be able to manage user state.
Assessment criteria
The learner can: 2.1 create User State Migration Tool (USMT) XML files 2.2 customise USMT XML files 2.3 manage user accounts 2.4 configure user state virtualization 2.5 migrate user state 2.6 optimise storage usage.

Learning outcome
The learner will: 3. Be able to use Windows tools.
Assessment criteria
The learner can: 3.1 managing Windows Using Group Policy 3.2 implement Windows remote management 3.3 describe the tools to use for Windows management 3.4 manage Windows using command line-based tools.

Guidance
3.2 this could be PowerShell Remoting 3.4 this could be Powershell

Learning outcome
The learner will: 4. Be able to configure network connections.
Assessment criteria
The learner can: 4.1 configure a local area network (LAN) connection 4.2 implement automatic IP address allocation 4.3 implement name resolution 4.4 resolve network connectivity problems 4.5 implement wireless network connectivity 4.6 describe **wireless network connections.**

Range
4.1 (IPv4, IPv6) **Wireless network connections** (standards, technologies)

Learning outcome
The learner will: 5. Be able to configure resource access.
Assessment criteria
The learner can: 5.1 configure domain access for Windows devices 5.2 manage non-domain devices 5.3 configure workplace join 5.4 configure work folders.

Learning outcome
The learner will: 6. Be able to secure networks.
Assessment criteria
The learner can: 6.1 Describe network security threats 6.2 Mitigate threats to network security 6.3 Secure network traffic.

Learning outcome
The learner will: 7. Be able to manage file access.
Assessment criteria
The learner can: 7.1 manage **hard disks** 7.2 describe cloud-based storage services 7.3 manage file and folder access 7.4 manage shared folder access 7.5 configure file and folder compression 7.6 manage **printers.**

Range
hard disks (local, virtual) **printers** (local, network)

Learning outcome
The learner will: 8. Be able to secure Windows devices.
Assessment criteria
The learner can: 8.1 describe methods used for authentication in Windows 8.2 describe methods used for authorization in Windows 8.3 describe how to use local Group Policy Objects (GPOs) to secure Windows 8.4 create multiple local GPOs 8.5 secure data 8.6 configure User Account Control (UAC).

Range
8.5 with EFS and with BitLocker

Learning outcome
The learner will: 9. Be able to maintain Windows client computers.
Assessment criteria
The learner can: 9.1 optimise Windows performance 9.2 manage the Windows reliability 9.3 manage software updates.

Learning outcome
The learner will: 10. Be able to configure applications for Windows.
Assessment criteria
The learner can: 10.1 describe application deployment options 10.2 manage apps on a Windows based operating system 10.3 configure Internet browser settings 10.4 configure application restrictions.

Learning outcome
The learner will: 11. Be able to configure remote access.
Assessment criteria
The learner can: 11.1 configure Windows settings for mobile computing devices 11.2 configure Virtual Private Network (VPN) access 11.3 configure DirectAccess 11.4 configure remote desktop 11.5 configure remote assistance.

Learning outcome
The learner will: 12. Be able to configure desktop virtualisation.
Assessment criteria
The learner can: 12.1 describe a client hypervisor 12.2 create virtual machines 12.3 manage virtual hard disks 12.4 manage checkpoints.

Guidance
12.1 could be Hyper-V

Learning outcome
The learner will: 13. Be able to recover a Windows based operating system.
Assessment criteria
The learner can: 13.1 explain Windows recovery options 13.2 back up files 13.3 restore files.

Unit 634 Installing and configuring Windows based servers

UAN:	**H/507/0335**
Level:	3
Credit value:	11
GLH:	57
Aim:	This unit provides the skills and knowledge necessary to implement a core Windows Server infrastructure. A learner achieving this unit will have the ability to implement and configure Windows Server core services, such as Active Directory and the networking services. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Installing and Configuring Windows Server.

Learning outcome
The learner will: 1. Be able to deploy Windows based servers.
Assessment criteria
The learner can: 1.1 describe the features of a Window based server 1.2 describe the server management **tools** 1.3 plan for a server installation 1.4 configure a server.

Range
tools (development, testing, connecting)

Learning outcome
The learner will: 2. Understand domain controllers.
Assessment criteria
The learner can: 2.1 describe the structure of domain controller services 2.2 describe the purpose of domain controllers 2.3 explain how to install a domain controller.

Learning outcome
The learner will: 3. Be able to manage user accounts.
Assessment criteria
The learner can: 3.1 **manage accounts** 3.2 delegate permissions 3.3 explain how to automate user account management.

Range
manage (create, configure, troubleshooting) **accounts** (user, group, computer)

Learning outcome
The learner will: 4. Be able to implement Internet Protocol (IP).
Assessment criteria
The learner can: 4.1 describe the TCP/IP protocol suite 4.2 describe **IP addressing options** 4.3 determine a **subnet mask** 4.4 configure IP options 4.5 troubleshoot IP options 4.6 describe the benefits of IPv6 4.7 describe the **interoperability** between IPv4 and IPv6.

Range
IP addressing options (IPv4, IPv6) **subnet mask** (subnetting or supernetting) **Interoperability** (Coexistence, transition)

Learning outcome
The learner will: 5. Be able to implement Dynamic Host Configuration Protocols (DHCP).
Assessment criteria
The learner can: 5.1 **configure** DHCP **server roles** 5.2 manage a DHCP database 5.3 manage the DHCP server role.

Range
configure (Also includes securing server role) **server roles** (Also includes scopes)

Learning outcome
The learner will: 6. Be able to implement Domain Name Systems (DNS).
Assessment criteria
The learner can: 6.1 install DNS server services 6.2 configure DNS 6.3 **manage** DNS.

Range
manage (also includes DNS zones, creating host records and server cache)

Learning outcome
The learner will: 7. Be able to configure server storage.
Assessment criteria
The learner can: 7.1 describe storage technologies 7.2 **configure storage** 7.3 **configure shared files and folders** 7.4 configure a printer pool.

Range
Configure storage (also includes resizing volumes, redundant storage space) **Configure shared files and folder** (a file share, shadow copies, protection, security)

Learning outcome
The learner will: 8. Be able to manage group policy.
Assessment criteria
The learner can: 8.1 **manage** group policy objects 8.2 describe server operating system security 8.3 configure software application restriction policies 8.4 audit **system access.**

Range
manage (also includes creating group policy objects, implementing a central store for administrative templates, security, restrict running of unauthorised software, a firewall with advanced security) **system access** (domain logons, file system access)

Learning outcome
The learner will: 9. Be able to implement server virtualization.
Assessment criteria
The learner can: 9.1 describe virtualisation technologies 9.2 configure a virtual machine 9.3 manage virtual machine storage 9.4 **manage** virtual networks.

Range
manage (to also include configure)

Unit 634 Installing and configuring Windows based servers

Supporting information

Guidance

Configuration of any aspect of the server also requires installation
For learners to know the benefits of IPV6, they should also learn the features
1.4 this includes admin tasks.
3.3 automation should be through command line tools

Unit 635 Programming in HTML5 with JavaScript and CSS3

UAN:	**A/507/0275**
Level:	3
Credit value:	11
GLH:	43
Aim:	This unit is designed to provide an introduction to HTML5, CSS3, and JavaScript. The unit focuses on using HTML5/CSS3/JavaScript to implement programming logic, define and use variables, perform looping and branching, develop user interfaces, capture and validate user input, store data, and create well-structured application. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for the Programming in HTML5 with JavaScript and CSS3.

Learning outcome
The learner will: 1. Be able to create HTML5 pages.
Assessment criteria
The learner can: 1.1 describe basic **HTML5** 1.2 explain the structure of Cascading Style Sheets (CSS) 1.3 describe Integrated Development Environment (IDE) tools available for building Web applications 1.4 create static pages using features of HTML5 1.5 apply styling to the elements in an HTML5 page.

Range
HTML5 (elements, attributes)

Learning outcome
The learner will: 2. Be able to code using JavaScript.
Assessment criteria
The learner can: 2.1 explain the syntax of JavaScript 2.2 describe how to use JavaScript with HTML5 2.3 write JavaScript code that manipulates the HTML DOM 2.4 write JavaScript code that handles events 2.5 describe how to use jQuery to simplify code 2.6 describe the benefits of structuring JavaScript code 2.7 explain best practices for creating custom objects in JavaScript 2.8 describe how to extend objects to add functionality.

Learning outcome
The learner will: 3. Be able to create forms using HTML5.
Assessment criteria
The learner can: 3.1 create forms using HTML5 3.2 validate user input using HTML5 attributes 3.3 create feedback using HTML5 attributes 3.4 write JavaScript code to validate user input.

Learning outcome
The learner will: 4. Be able to communicate with a remote data source.
Assessment criteria
The learner can: 4.1 communicate data by using **XMLHttpRequest** objects 4.2 simplify code that communicates data using the jQuery ajax method.

Range
XMLHttpRequest (has member types: Events, Methods, Properties)

Learning outcome
The learner will: 5. Be able to style HTML5 by using CSS3.
Assessment criteria
The learner can: 5.1 style text elements on an HTML5 page by using CSS3 5.2 apply styling to block elements by using CSS3 5.3 use CSS3 selectors to specify the elements to be styled in a Web application 5.4 implement effects by using **CSS3 properties**.

Range
CSS3 properties (graphical, transformations)

Learning outcome
The learner will: 6. Be able to create interactive pages using HTML5 Application Programming Interfaces (APIs).
Assessment criteria
The learner can: 6.1 use APIs to interact with files in a Web application 6.2 incorporate media into a **Web application** 6.3 detect the location of the user running a Web application 6.4 explain how to debug a Web application 6.5 explain how to profile a Web application.

Range
Web application (video, audio)

Learning outcome
The learner will: 7. Be able to add offline support to web applications.
Assessment criteria
The learner can: 7.1 save data locally on the user's computer 7.2 retrieve data locally on the user's computer 7.3 incorporate offline support for a Web application.

Learning outcome
The learner will: 8. Be able to implement an adaptive User Interface (UI).
Assessment criteria
The learner can: 8.1 describe the need for a Web application to detect device capabilities 8.2 describe the need for a Web application to react to different form factors 8.3 create a Web page that can dynamically adapt its layout to match different form factors.

Learning outcome
The learner will: 9. Be able to create graphics.
Assessment criteria
The learner can: 9.1 add interactive graphics to an **application** 9.2 draw complex graphics on an HTML5 Canvas element by using JavaScript code.

Range
application (guidance using Scalable Vector Graphics)

Learning outcome
The learner will: 10. Be able to animate the User Interface (UI).
Assessment criteria
The learner can: 10.1 describe the types of transitions available with CSS3 10.2 apply CSS transitions to elements on an HTML5 page 10.3 implement complex **animations** 10.4 write JavaScript code to detect when a transition has occurred.

Range
animations (using CSS key-frames, using JavaScript code)

Learning outcome
The learner will: 11. Be able to implement Real-Time communications by using Web sockets.
Assessment criteria
The learner can: 11.1 explain how Web Sockets work 11.2 describe how to communicate data through a Web Socket 11.3 use the Web Socket API with JavaScript to **communicate** with a Web Socket server.

Range
communicate (send and receive data, and handle the different events that can occur when a message is sent or received)

Learning outcome
The learner will: 12. Be able to create a Web Worker process.
Assessment criteria
The learner can: 12.1 describe the **purpose** of a Web Worker process 12.2 use the Web Worker APIs from JavaScript code for a Web Worker **process**.

Range
purpose (perform asynchronous processing, provide isolation for sensitive operations) **process** (create, run, and monitor

Unit 636 Implementing a Windows based data warehouse

UAN:	**T/507/0338**
Level:	3
Credit value:	10
GLH:	41
Aim:	This unit is aimed at those who will be involved in Extract Transform Load (ETL) and data warehouse development creating Business Intelligence (BI) solutions and have some responsibilities for data cleansing and data warehouse implementation. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for SQL Bi Development.

Learning outcome
The learner will: 1. Understand the requirements for data warehouse hardware.
Assessment criteria
The learner can: 1.1 describe the main hardware considerations for building a data warehouse 1.2 explain how to use reference architectures to create a data warehouse 1.3 explain how to use data warehouse appliances to create a data warehouse.

Learning outcome
The learner will: 2. Be able to implement a data warehouse.
Assessment criteria
The learner can: 2.1 describe the key elements of a data warehousing solution 2.2 describe the key considerations for a data warehousing project 2.3 implement a logical design for a data warehouse 2.4 implement a physical design for a data warehouse.

Learning outcome
The learner will: 3. Be able to create an Extract, Transform and Load (ETL) Solution.
Assessment criteria
The learner can: 3.1 describe the key features of SQL Server Integration Services (SSIS) 3.2 explore source data for an ETL solution 3.3 implement a data flow using SSIS 3.4 implement control flow with **constraints** 3.5 create dynamic packages 3.6 use containers in a package control flow 3.7 enforce **consistency** 3.8 manage an **SSIS package**.

Range
constraints (tasks, precedence) **consistency** (with transactions, with checkpoints) **SSIS package** (debug, logging, error handling

Learning outcome
The learner will: 4. Be able to implement an incremental ETL process.
Assessment criteria
The learner can: 4.1 describe the considerations for implementing an incremental ETL solution 4.2 extract data from source systems 4.3 insert data into a data warehouse.

Learning outcome
The learner will: 5. Be able use a cloud data warehousing solution.
Assessment criteria
The learner can: 5.1 describe cloud data scenarios 5.2 describe cloud database software 5.3 implement a **cloud-based database.**

Range
cloud-based database (guidance create, extract and obtain data from cloud services)

Learning outcome
The learner will: 6. Be able to use Data Quality Services (DQS).
Assessment criteria
The learner can: 6.1 describe how DQS can help manage data quality 6.2 use DQS to cleanse data 6.3 use DQS to match data.

Learning outcome
The learner will: 7. Be able to use Master Data Services.
Assessment criteria
The learner can: 7.1 describe key Master Data Services concepts 7.2 implement a Master Data Services model 7.3 use the Master Data Services **add-in for spreadsheets.**

Range
add-in for spreadsheets (to view a model, to modify a model) (guidance Excel for spreadsheet)

Learning outcome
The learner will: 8. Be able to use SSIS packages.
Assessment criteria
The learner can: 8.1 describe how custom components can be used to extend SSIS 8.2 describe how to use custom scripts in an SSIS package 8.3 describe SSIS deployment 8.4 plan SSIS package execution.

Learning outcome
The learner will: 9. Understand Business Intelligence (BI).
Assessment criteria
The learner can: 9.1 describe BI scenarios 9.2 explain the key features of SQL Server Reporting Services 9.3 explain the key features of SQL Server Analysis Services.

Unit 637 Managing a Windows based system

UAN:	**A/507/0342**
Level:	3
Credit value:	11
GLH:	49
Aim:	Candidates for this exam are IT professionals who configure or support Windows computers, devices, users, and associated network and security resources. The networks with which these professionals typically work are configured as domain-based or peer-to-peer environments with access to the Internet and cloud services. The IT professional could be a consultant, a full-time desktop support technician, or an IT generalist who administers Windows based computers and devices as a portion of their broader technical responsibilities.

Learning outcome
The learner will: 1. Be able to implement management of a Windows based operating system.
Assessment criteria
The learner can: 1.1 perform local management of Windows 1.2 perform remote management of Windows 1.3 manage Windows using Group Policy 1.4 describe management tools for Windows.

Guidance
1.2 this could be PowerShell

Learning outcome
The learner will: 2. Be able to implement an installation strategy.
Assessment criteria
The learner can: 2.1 determine a Windows deployment strategy 2.2 implement a Windows migration strategy 2.3 plan Windows deployment methods 2.4 implement Windows deployment methods 2.5 plan for operating system virtualisation 2.6 create an unattended answer file 2.7 modify a Windows image offline 2.8 configure boot to Virtual Hard Drive (VHD).

Learning outcome
The learner will: 3. Be able to implement Windows authentication.
Assessment criteria
The learner can: 3.1 plan user authentication 3.2 plan domain-based security 3.3 implement authentication 3.4 troubleshoot domain authentication.

Learning outcome
The learner will: 4. Be able to implement intranet connectivity.
Assessment criteria
The learner can: 4.1 describe methods for obtaining IPv4 configurations 4.2 plan intranet connectivity 4.3 configure IPv4 4.4 describe how name resolution works 4.5 describe tools for troubleshooting network issues 4.6 troubleshoot common network issues.

Learning outcome
The learner will: 5. Be able to implement an application strategy for Windows.
Assessment criteria
The learner can: 5.1 manage application installers 5.2 design application deployment 5.3 plan an application compatibility strategy 5.4 manage applications.

Learning outcome
The learner will: 6. Be able to implement a solution for user settings.
Assessment criteria
The learner can: 6.1 plan a solution for implementation of user settings 6.2 manage user profiles 6.3 explain User Experience Virtualization (UE-V) 6.4 deploy UE-V.

Learning outcome
The learner will: 7. Be able to configure access to cloud service.
Assessment criteria
The learner can: 7.1 describe **cloud services** that support Windows management 7.2 plan for cloud services deployment 7.3 deploy cloud services 7.4 configure Windows cloud based services.

Range
cloud services (purpose, functionality, policies, updates)

Learning outcome
The learner will: 8. Be able to implement access to file and print services.
Assessment criteria
The learner can: 8.1 manage local storage 8.2 implement access to files 8.3 implement access to file shares 8.4 implement file caching 8.5 plan client-side printing 8.6 configure client-side printing.

Learning outcome
The learner will: 9. Be able to implement encryption for Windows.
Assessment criteria
The learner can: 9.1 plan the implementation of an Encrypting File System (EFS) 9.2 plan the use of BitLocker 9.3 implement BitLocker 9.4 manage BitLocker.

Learning outcome
The learner will: 10. Be able to implement endpoint security.
Assessment criteria
The learner can: 10.1 plan endpoint security 10.2 implement centralised configuration for Windows updates 10.3 implement Windows cloud services endpoint protection 10.4 configure applications restrictions.

Learning outcome
The learner will: 11. Be able to implement extranet connectivity.
Assessment criteria
The learner can: 11.1 explain how DirectAccess provides seamless remote access to intranet resources 11.2 configure Virtual Private Network (VPN) Access 11.3 manage mobile device connectivity to extranet.

Learning outcome
The learner will: 12. Be able to implement recovery solutions.
Assessment criteria
The learner can: 12.1 plan a recovery solution 12.2 diagnose problems with the Windows boot process 12.3 repair Windows stability issues 12.4 implement a user data recovery strategy for Windows.

Unit 638 Designing and implementing a Windows desktop infrastructure

UAN:	**T/507/0341**
Level:	4
Credit value:	13
GLH:	56
Aim:	This unit provides the skills and knowledge necessary for designing, implementing, and maintaining a Windows server desktop infrastructure. A learner achieving this unit will have the ability to plan, configure, and implement the Windows based Server desktop services, such as desktop imaging and deployment, application/desktop virtualization, and RDP access and infrastructure. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Managing Modern Desktops.

Learning outcome
The learner will: 1. Understand desktop deployment options.
Assessment criteria
The learner can: 1.1 describe the enterprise desktop life cycle 1.2 explain how to assess readiness for a desktop deployment 1.3 describe the available methods for deploying enterprise desktops 1.4 describe volume activation technologies for enterprise desktops 1.5 plan a desktop deployment strategy 1.6 implement a volume activation solution.

Learning outcome
The learner will: 2. Understand how to plan an image management strategy.
Assessment criteria
The learner can: 2.1 determine the type of **images** used in an image management strategy 2.2 determine the content of images used in an image management strategy 2.3 assess business requirements to support an image management strategy.

Learning outcome
The learner will: 3. Be able to implement desktop security.
Assessment criteria
The learner can: 3.1 implement a centralised secure desktop solution by using Group Policy settings 3.2 plan device encryption by using BitLocker 3.3 implement device encryption by using BitLocker 3.4 plan a centrally managed EFS solution 3.5 implement a centrally managed EFS solution 3.6 configure desktop security.

Learning outcome
The learner will: 4. Be able to manage a desktop operating system image.
Assessment criteria
The learner can: 4.1 identify the key features of the Windows *ADK* 4.2 describe the Windows *PE* environment 4.3 describe how answer files are used in Windows installations 4.4 capture a reference image 4.5 service a reference image 4.6 configure Windows DS 4.7 configure a custom windows PE environment 4.8 build a custom answer file 4.9 generalise a reference computer 4.10 configure Windows deployment services server role.

Range
4.6 for image capture and for image deployment

Learning outcome
The learner will: 5. Be able to implement user state migration.
Assessment criteria
The learner can: 5.1 plan user state migration 5.2 migrate user state by using the User State Migration Tool (USMT) 5.3 create USMT XML Files 5.4 customise USMT XML Files.

Learning outcome
The learner will: 6. Be able to design an Active Directory Domain Services physical infrastructure.
Assessment criteria
The learner can: 6.1 plan for the LTI environment 6.2 implement MDT for LTI 6.3 integrate Windows Deployment Services (DS) with the MDT 6.4 plan the ZTI environment 6.5 prepare the site for operating system deployment 6.6 build a reference image by using a configuration manager task sequence 6.7 deploy client images by using MDT task sequences.

Learning outcome
The learner will: 7. Be able to implement a remote desktop services infrastructure.
Assessment criteria
The learner can: 7.1 plan the Remote Desktop Services environment 7.2 configure desktop deployments 7.3 extend the Remote Desktop Services environment to the Internet.

Range
7.2 for virtual machine–based and session-based

Learning outcome
The learner will: 8. Be able to manage user state virtualization for enterprise desktops.
Assessment criteria
The learner can: 8.1 describe considerations for implementing an enterprise-based updates infrastructure 8.2 describe how to use System Center Configuration Manager for software updates 8.3 describe how to manage software updates 8.4 describe how to configure Windows Intune for software updates 8.5 determine software update compliance 8.6 deploy software updates to clients.

Range
8.2 deploy, manage 8.3 for virtual machine, for images 8.4 deploy, manage

Learning outcome
The learner will: 9. Be able to design network access services.
Assessment criteria
The learner can: 9.1 design remote access services 9.2 implement remote access services 9.3 design a perimeter network.

Guidance
9.1 and 9.2 Remote Authentication Dial-In User Service (RADIUS), DirectAccess

Learning outcome
The learner will: 10. Be able to protect enterprise desktops.
Assessment criteria
The learner can: 10.1 configure System Center Endpoint Protection 10.2 describe how to use Windows Intune endpoint protection 10.3 describe how to protect desktops by using DPM 10.4 monitor endpoint protection 10.5 configure client data protection.

Guidance
10.1 to include protection point, protection policies, client settings, monitoring status

Learning outcome
The learner will: 11. Be able to monitor the performance of the desktop infrastructure.
Assessment criteria
The learner can: 11.1 configure performance monitoring of desktops 11.2 configure reliability monitoring of desktops 11.3 configure operations manager for monitoring virtual environments 11.4 monitor the desktop infrastructure.

Guidance
11.4 to include health, performance and VDI

Unit 639 Implementing Windows desktop application environments

UAN:	**M/507/0340**
Level:	4
Credit value:	12
GLH:	50
Aim:	This unit provides the skills and knowledge necessary to design, implement, and maintain a Windows Server desktop infrastructure. A learner achieving this unit will have the ability to plan, configure, and implement the Windows Server desktop services, such as desktop imaging and deployment, application/desktop virtualisation, and RDP access and infrastructure This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Managing Modern Desktops.

Learning outcome
The learner will: 1. Be able to design an application distribution strategy.
Assessment criteria
The learner can: 1.1 describe how to develop an application lifecycle strategy 1.2 describe the factors affecting application distribution design 1.3 design an application distribution strategy.

Learning outcome
The learner will: 2. Be able to resolve application compatibility.
Assessment criteria
The learner can: 2.1 explain considerations for diagnosing application compatibility issues 2.2 explain solutions available for remediating application compatibility issues 2.3 resolve application compatibility issues with the Application Compatibility Toolkit (ACT).

Learning outcome
The learner will: 3. Be able to deploy software.
Assessment criteria
The learner can: 3.1 deploy software 3.2 install Windows apps using sideloading.

Range
3.1 centrally using Group Policy, to clients

Learning outcome
The learner will: 4. Be able to configure self-service applications.
Assessment criteria
The learner can: 4.1 plan self-service application deployment 4.2 configure self-service application deployment 4.3 describe how to improve the self-service application deployment process.

Learning outcome
The learner will: 5. Be able to implement presentation virtualisation infrastructure.
Assessment criteria
The learner can: 5.1 describe how to assess presentation virtualisation requirements 5.2 describe how to plan presentation virtualisation infrastructure 5.3 describe how to extend presentation virtualisation infrastructure 5.4 assess capacity requirements for presentation virtualisation 5.5 configure presentation virtualisation infrastructure.

Range
5.5 to include high availability, remote access)

Learning outcome
The learner will: 6. Be able to deploy presentation virtualisation applications.
Assessment criteria
The learner can: 6.1 determine a presentation virtualisation application strategy 6.2 plan how to deploy applications to Remote Desktop Session Host (RD Session Host) servers 6.3 deploy applications to RD Session Host servers 6.4 configure access to RD Session Host resources 6.5 deploy RD Session Host desktop applications 6.6 configure remote applications 6.7 verify remote applications.

Learning outcome
The learner will: 7. Be able to deploy an application virtualisation environment.
Assessment criteria
The learner can: 7.1 determine an application virtualisation model to meet business requirements 7.2 deploy components to support an application virtualisation model 7.3 deploy the Windows application virtualisation client 7.4 configure the Windows application virtualisation client.

Learning outcome
The learner will: 8. Be able to deploy virtual applications.
Assessment criteria
The learner can: 8.1 configure the Windows Application Virtualisation Sequencer 8.2 sequence applications 8.3 deploy sequenced applications deploy software updates to clients.

Learning outcome
The learner will: 9. Be able to implement application updates.
Assessment criteria
The learner can: 9.1 plan application updates 9.2 deploy application updates 9.3 implement application update security.

Learning outcome
The learner will: 10. Be able to implement application upgrades.
Assessment criteria
The learner can: 10.1 plan application upgrades 10.2 implement application upgrades 10.3 plan application concurrency 10.4 implement application concurrency 10.5 configure application version coexistence.

Guidance
10.1 upgrades would naturally include supersedense

Learning outcome
The learner will: 11. Know how to monitor application deployment.
Assessment criteria
The learner can: 11.1 describe how to plan application monitoring 11.2 describe how to plan **software monitoring** 11.3 describe how to monitor application resource use 11.4 configure server monitoring.

Guidance
11.2 **software monitoring** (inventory and metering)

Unit 640 Supporting Microsoft Exchange server solutions

UAN:	**J/507/0344**
Level:	4
Credit value:	12
GLH:	52
Aim:	This unit is designed to provide learners with the knowledge and skills to plan, deploy, manage, secure, and support Microsoft Exchange Server. It covers monitoring, maintaining, and troubleshooting an Exchange Server that will include guidelines, best practices, and considerations to help optimize performance and minimize errors and security threats. This is an ideal for those aspiring to be enterprise-level messaging administrators, though it would also benefit those seeking a career as an IT generalist and or help desk professional. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Designing and Developing Exchange Server.

Learning outcome
The learner will: 1. Be able to manage Microsoft Exchange Server.
Assessment criteria
The learner can: 1.1 describe Exchange Server prerequisites 1.2 deploy an Exchange Server 1.3 manage Exchange Server 1.4 evaluate requirements for an Exchange Server installation 1.5 monitor Exchange Server 1.6 maintain Exchange Server 1.7 troubleshoot Exchange Server.

Learning outcome
The learner will: 2. Be able to configure Mailbox Servers.
Assessment criteria
The learner can: 2.1 describe the Mailbox Server role 2.2 plan for a Mailbox Server role deployment 2.3 configure the Mailbox Server 2.4 configure Storage on the Mailbox Server 2.5 configure Mailbox Databases.

Learning outcome
The learner will: 3. Be able to manage recipient objects.
Assessment criteria
The learner can: 3.1 manage Exchange Server mailboxes 3.2 manage Exchange Server recipients 3.3 implement public folders 3.4 configure address lists 3.5 configure policies.

Learning outcome
The learner will: 4. Be able to configure self-service applications.
Assessment criteria
The learner can: 4.1 plan self-service application deployment 4.2 configure self-service application deployment 4.3 describe how to improve the self-service application deployment process.

Learning outcome
The learner will: 5. Be able to configure messaging client connectivity.
Assessment criteria
The learner can: 5.1 describe the Exchange Server client services 5.2 configure messaging client web Application 5.3 plan mobile messaging 5.4 configure mobile messaging 5.5 configure secure Internet access for Client Access server.

Learning outcome
The learner will: 6. Be able to configure high availability.
Assessment criteria
The learner can: 6.1 describe a highly available Exchange Server 6.2 configure highly available Mailbox Databases 6.3 configure highly available Client Access servers.

Learning outcome
The learner will: 7. Be able to implement disaster recovery.
Assessment criteria
The learner can: 7.1 plan disaster mitigation 7.2 plan Exchange Server backup 7.3 implement Exchange Server backup 7.4 plan Exchange Server recovery 7.5 implement Exchange Server recovery.

Learning outcome
The learner will: 8. Be able to deploy virtual applications.
Assessment criteria
The learner can: 8.1 describe how message transport operates in Exchange Server 8.2 plan message transport 8.3 configure message transport 8.4 manage transport rules.

Learning outcome
The learner will: 9. Be able to implement message security.
Assessment criteria
The learner can: 9.1 plan messaging security 9.2 implement an antivirus solution for Exchange Server 9.3 implement an anti-spam solution for Exchange Server.

Learning outcome
The learner will: 10. Be able to configure administrative security.
Assessment criteria
The learner can: 10.1 configure Role Based Access Control (RBAC) permissions 10.2 configure audit logging.

Unit 641 Designing and implementing a Windows server infrastructure

UAN:	**M/507/0337**
Level:	4
Credit value:	13
GLH:	54
Aim:	This unit provides the skills and knowledge necessary design, implement, and maintain a Windows based server infrastructure. A learner achieving this unit will have the ability to plan, configure, and implement Windows based Server services, such as server deployment, server virtualization, and network access and infrastructure. This unit is linked to the Microsoft Official Academic Course (MOAC) and Exam for Designing and Implementing a Server Infrastructure.

Learning outcome
The learner will: 1. Understand how to plan a server upgrade or migration.
Assessment criteria
The learner can: 1.1 describe server upgrade considerations 1.2 describe server migration considerations 1.3 explain how to plan for server virtualisation 1.4 plan a server upgrade and migration strategy.

Learning outcome
The learner will: 2. Be able to implement a server deployment strategy.
Assessment criteria
The learner can: 2.1 explain how to plan for an automated server installation and deployment strategy 2.2 determine a deployment automation strategy 2.3 implement an automated deployment strategy.

Learning outcome
The learner will: 3. Be able to implement an address management solution.
Assessment criteria
The learner can: 3.1 design a Dynamic Host Configuration Protocol (DHCP) strategy 3.2 implement DHCP strategy.

Guidance
3.1 and 3.2 to include DNCP scope configuration, IP address management (IPAM))

Learning outcome
The learner will: 4. Be able to implement a name resolution strategy.
Assessment criteria
The learner can: 4.1 design a Domain Name System (DNS) server implementation strategy 4.2 implement a DNS zone strategy 4.3 configure DNS zone replication 4.4 optimise the DNS server configuration.

Guidance
4.1 to include DNS namespace, DNS zone strategy, DNS zone replication, DNS for high availability and security

Learning outcome
The learner will: 5. Be able to implement Active Directory Domain Services logical infrastructures.
Assessment criteria
The learner can: 5.1 design an Active Directory Domain Services (AD DS) infrastructure 5.2 implement an Active Directory Domain Services (AD DS) infrastructure 5.3 plan an AD DS administrative tasks delegation model 5.4 design an Organizational Unit (OU) structure 5.5 design an AD DS group strategy 5.6 implement an AD DS group strategy 5.7 determine information required to facilitate a Group Policy Object (GPO) design 5.8 analyse the information required to facilitate a GPO design 5.9 create a GPO design 5.10 implement a GPO design.

Guidance
5.1 and 5.2 to include forest, forest trusts, domains, domain trusts, namespaces

Learning outcome
The learner will: 6. Be able to design an Active Directory Domain Services physical infrastructure.
Assessment criteria
The learner can: 6.1 design AD DS sites 6.2 design AD DS replication 6.3 design domain controller placement 6.4 design domain controller deployments 6.5 implement active directory sites 6.6 implement domain controllers.

Guidance
6.4 to include highly available and on virtual machines

Learning outcome
The learner will: 7. Be able to implement storage.
Assessment criteria
The learner can: 7.1 plan a **storage solution** 7.2 implement a storage solution 7.3 configure redundant storage space.

Range
storage solution (storage spaces, efficient storage, Internet Small Computer System Interface (iSCSI) storage area network (SAN))

Learning outcome
The learner will: 8. Be able to implement file services.
Assessment criteria
The learner can: 8.1 plan a Distributed File System (DFS) 8.2 implement a DFS 8.3 plan Windows BranchCache 8.4 implement Windows BranchCache 8.5 plan Dynamic Access Control 8.6 implement Dynamic Access Control.

Learning outcome
The learner will: 9. Be able to design network access services.
Assessment criteria
The learner can: 9.1 design **remote access services** 9.2 implement remote access services 9.3 design a perimeter network.

Range
remote access services (Remote Authentication Dial-In User Service (RADIUS), DirectAccess

Learning outcome
The learner will: 10. Be able to design network protection.
Assessment criteria
The learner can: 10.1 design **network security** 10.2 implement network security 10.3 identify network security threats 10.4 describe how to mitigate network security threats.

Range
network security (Windows Firewall, Network Access Protection (NAP))

Unit 642 Creating an event-driven computer program

UAN:	**F/601/3179**
Level:	3
Credit value:	12
GLH:	90
Aim:	This unit covers more advanced concepts of event-driven computer languages and their use to implement, refine and test computer programs.

Learning outcome
The learner will: 1. Implement a software design using event-driven programming.
Assessment criteria
The learner can: 1.1 Identify the screen components and data and file structures required to implement a given design 1.2 Select, declare and initialise variable and data structure types and sizes to implement design requirements 1.3 Select and assign properties to screen components to implement design requirements 1.4 Select and associate events (including parameter passing) to 1.5 screen components to implement design requirements 1.6 Select and declare file structures to meet design file storage requirements 1.7 Select and use standard input/output commands to implement design requirements 1.8 Make effective use of operators and predefined functions 1.9 Make effective use of an integrated development environment (IDE) including code and screen templates.

Learning outcome
The learner will: 2. Refine an event-driven program to improve quality.
Assessment criteria
The learner can: 2.1 Use an agreed standard for naming, comments and code layout determine a deployment automation strategy 2.2 Define user functions to replace repeating code sequences 2.3 Implement data validation for inputs 2.4 Identify and implement opportunities for error handling and reporting.

Learning outcome
The learner will: 3. Test the operation of an event-driven program.
Assessment criteria
The learner can: 3.1 Make effective use of the debugging facilities available in the IDE 3.2 Prepare a test strategy 3.3 Select suitable test data and determine expected test results 3.4 Record actual test results to enable comparison with expected results 3.5 Analyse actual test results against expected results to identify discrepancies 3.6 Investigate test discrepancies to identify and rectify their causes.

Learning outcome
The learner will: 4. Document an event-driven program.
Assessment criteria
The learner can: 4.1 Create on-screen help to assist the users of a computer program implement a DNS zone strategy 4.2 Create documentation for the support and maintenance of a computer programme

Unit 644 Creating an object-oriented computer program

UAN:	**L/601/3184**
Level:	3
Credit value:	12
GLH:	90
Aim:	This unit covers more advanced concepts of object-oriented computer languages and their use to implement, refine and test computer programs.

Learning outcome
The learner will: 1. Implement a software design using object-oriented programming
Assessment criteria
The learner can: 1.1 Identify the objects and data and file structures required to implement a given design 1.2 Select, declare and initialise variable and data structure types and sizes to implement design requirements 1.3 Define relationships between objects to implement design requirements 1.4 Implement message passing between objects to implement design requirements 1.5 Implement object behaviours using control structures to meet the design algorithms 1.6 Select and declare file structures to meet design file storage requirements 1.7 Select and use standard input/output commands to implement design requirements 1.8 Make effective use of operators and predefined functions 1.9 Make effective use of an Integrated Development Environment (IDE) including code and screen templates.

Learning outcome
The learner will: 2. Refine an object-oriented program to improve quality
Assessment criteria
The learner can: 2.1 Use an agreed standard for naming, comments and code layout 2.2 Make effective use of encapsulation, polymorphism and inheritance 2.3 Implement data validation for inputs 2.4 Identify and implement opportunities for error handling and reporting.

Learning outcome
The learner will: 3. Test the operation of an object-oriented driven program
Assessment criteria
The learner can: 3.1 Make effective use of the debugging facilities available in the IDE 3.2 Prepare a test strategy 3.3 Select suitable test data and determine expected test results 3.4 Record actual test results to enable comparison with expected results 3.5 Analyse actual test results against expected results to identify discrepancies 3.6 Investigate test discrepancies to identify and rectify their causes.

Learning outcome
The learner will: 4. Document an object-oriented driven program
Assessment criteria
The learner can: 4.1 Create on-screen help to assist the users of a computer program 4.2 Create documentation for the support and maintenance of a computer program.

Unit 857 Principles of information governance and assurance

UAN:	**K/505/5786**
Level:	3
Credit value:	15
GLH:	75
Aim:	This unit develops the knowledge and skills required to implement information governance. Upon completion of this unit, learners will have an understanding of the procedures involved in implementing information governance and the legislation that must be complied with.

Learning outcome
The learner will: 1. Understand the purpose of information governance.
Assessment criteria
The learner can: 1.1 explain the importance of confidentiality, integrity and availability for information systems 1.2 explain the role of identity in information security 1.3 explain the importance and use of cryptographic techniques in information security 1.4 describe the information security procedures required by different types of organisations 1.5 outline the legal requirements for information security for individuals and organisations.

Learning outcome
The learner will: 2. Understand information security threats and vulnerabilities.
Assessment criteria
The learner can: 2.1 describe the types of threats facing the information security of individuals and organisations 2.2 explain the development of threats to the information security of individuals and organisations 2.3 describe sources of threats to information security in terms of opportunity, ability and motive 2.4 describe the types of information security vulnerabilities that can arise in hardware and software components 2.5 explain how hardware and software vulnerabilities can be identified and resolved.

Learning outcome
The learner will: 3. Understand information security techniques and technologies.
Assessment criteria
The learner can: 3.1 describe common cryptographic techniques including examples of their use in information security 3.2 explain the limitations of cryptography and their impact on information security 3.3 explain how physical and logical access controls can be used to protect information systems 3.4 design an access control system incorporating levels of access and the use of identity to protect a given information asset 3.5 compare proactive and reactive information security techniques 3.6 explain the information security features of hardware and network components 3.7 compare ethical and unethical hacking 3.8 describe how ethical hacking can contribute to information security testing.

Learning outcome
The learner will: 4. Understand information security risk assessment and management.
Assessment criteria
The learner can: 4.1 describe how to identify information assets which may be at risk 4.2 assess the probability and impact of given risks 4.3 describe available methods for preserving and restoring the integrity and availability of information assets 4.4 explain the responsibilities of system users for information security.

Unit 858 Testing the security of information systems

UAN:	**T/505/5788**
Level:	3
Credit value:	12
GLH:	40
Aim:	This unit aims to develop the knowledge and skills required to test the information security implemented on a system to establish its effectiveness. Upon completion of this unit, learners will be able to plan and carry out the security testing of information systems.

Learning outcome
The learner will: 1. Be able to conduct security testing.
Assessment criteria
The learner can: 1.1 develop test scripts for specified information assurance requirements testing 1.2 create plans that ensure that specified information assurance requirements are tested 1.3 implement specified preparations prior to carrying out tests 1.4 apply specified test methods, tools and techniques following organisational procedures 1.5 record the results of tests using standard documentation 1.6 implement specified activities following the completion of testing.

Learning outcome
The learner will: 2. Be able to report on test results.
Assessment criteria
The learner can: 2.1 examine the results of testing to identify security vulnerabilities 2.2 prioritise identified vulnerabilities against specified information assurance requirements 2.3 report any high priority vulnerabilities to the relevant persons following organisational procedures 2.4 identify the type of actions required to mitigate identified vulnerabilities 2.5 report the results of test activities using standard documentation following organisational procedures.

Unit 859 Carrying out information security risk assessment

UAN:	**T/505/5791**
Level:	3
Credit value:	9
GLH:	30
Aim:	This unit develops the knowledge and skills required to assess information security risks. Learners achieving this unit will be able to gather information that can be used to develop information security risk contingency plans and manage the identified risks.

Learning outcome
The learner will: 1. Be able to gather information on information security risks.
Assessment criteria
The learner can: 1.1 verify the scope of information assets and system components to be assessed with relevant persons 1.2 use specified investigative methods following organisational procedures 1.3 gather information to enable the security of specified information assets and system components to be assessed 1.4 record all gathered information using standard documentation.

Learning outcome
The learner will: 2. Be able to assess and report on information security risks.
Assessment criteria
The learner can: 2.1 examine gathered information to identify risks to the security of specified information assets and system components 2.2 categorise the priority of identified risks by determining their probability of occurrence and potential impact 2.3 report high priority risks to the relevant persons following organisational procedures 2.4 determine the types of actions required to mitigate identified risks 2.5 report the results of risk assessment activities using standard documentation following organisational procedures.

Unit 860 Investigating information security incidents

UAN:	**F/505/5793**
Level:	3
Credit value:	9
GLH:	23
Aim:	This unit aims to develop the knowledge and skills required to investigate a security incident. Upon completion of this unit, learners will be able to gather information that can be used to determine the impact of a security incident and make recommendations regarding the mitigation of the associated risks.

Learning outcome
The learner will: 1. Be able to gather information to investigate information security incidents.
Assessment criteria
The learner can: 1.1 identify the information assets and system components that may be impacted by detected incidents 1.2 verify the scope of detected incidents with relevant persons 1.3 obtain and preserve evidence relating to detected incidents.

Learning outcome
The learner will: 2. Be able to investigate information security incidents.
Assessment criteria
The learner can: 2.1 undertake agreed investigative actions 2.2 examine how access to the affected information assets and system components was obtained 2.3 report to the relevant persons any incidents for which the mode of access cannot be identified 2.4 make recommendations on the need for detailed forensic examinations 2.5 report on incident investigation activities using standard documentation 2.6 follow organisational procedures for investigation activities.

Unit 862 Carrying out information security incident management activities

UAN:	**F/505/5812**
Level:	3
Credit value:	9
GLH:	25
Aim:	This unit aims to develop the knowledge and skills required to manage information security risks., Learners will be able to gather information that can be used to develop information security risk contingency plans and manage the identified risks.

Learning outcome
The learner will: 1. Be able to gather information to manage information security incidents.
Assessment criteria
The learner can: 1.1 follow organisational procedures for the detection and classification of incidents 1.2 identify the information assets and system components that may be impacted by detected incidents 1.3 verify the scope of detected incidents with relevant persons 1.4 obtain information and data on incidents to assess their impact on information assets and system components.

Learning outcome
The learner will: 2. Be able to carry out information security incident management activities.
Assessment criteria
The learner can: 2.1 identify types of actions required to resolve incidents or mitigate their impact 2.2 report any incidents which cannot be resolved or mitigated to the relevant persons following organisational procedures 2.3 make recommendations for specific actions to be taken to respond to incidents 2.4 report on incident management activities using standard documentation following organisational procedures 2.5 follow organisational procedures for the closure of incidents.

Unit 863 Carrying out information security forensic examinations

UAN:	**R/505/5801**
Level:	3
Credit value:	6
GLH:	10
Aim:	This unit develops in learners the knowledge and skills required to undertake forensic examinations following an issue involving information, to ensure that evidence is preserved. Learners achieving this unit will know how to carry out the actions required to prevent evidence being compromised by activities undertaken when investigating an issue involving information security.

Learning outcome
The learner will: 1. Be able to carry out information security forensic examinations.
Assessment criteria
The learner can: 1.1 follow organisational procedures for forensic examinations 1.2 undertake specified actions to secure information assets and system components subject to actual or attempted breaches of security 1.3 apply forensic methods to examine specified system information for evidence of actual or attempted breaches of security policy or legislation 1.4 report any identified sources of actual or attempted breaches of security to the relevant persons 1.5 use specified tools to analyse the integrity of software 1.6 report on forensic examination activities using standard documentation.

Unit 865 Carrying out information security audits

UAN:	**A/505/5808**
Level:	3
Credit value:	6
GLH:	10
Aim:	This unit provides the skills and knowledge necessary to plan and undertake information security audits. Upon completion of this unit, learners will be able to plan and undertake security audits that can be used to manage any identified risks.

Learning outcome
The learner will: 1. Be able to carry out information security audit activities.
Assessment criteria
The learner can: 1.1 verify the scope of information assets and system components to be audited with relevant persons 1.2 use specified audit methods to obtain information and data relating to information assets and system components to assess security compliance 1.3 examine information and data relating to information assets and system components to assess security compliance 1.4 report any security non-compliance to the relevant persons 1.5 report on audit activities using standard documentation 1.6 follow organisational procedures for information security audits.

Unit 868 User profile administration

UAN:	**K/500/7379**
Level:	3
Credit value:	9
GLH:	80
Aim:	This unit provides the underpinning knowledge to enable learners to configure and administer user profiles. Upon completion of this unit, learners will understand types of user profiles and how to assign permissions.

Learning outcome
The learner will: 1. Know how to administer user profiles.
Assessment criteria
The learner can: 1.1 describe the organisational policy on user profiles, such as: a user identifier (eg. username) b password and related information (eg change frequency) c allowed system access (eg times, locations) d allowed access to facilities (eg data, software) 1.2 describe how to create and edit user and standard profiles 1.3 describe how user profiles affect access to system facilities, such as a shared resources (eg data storage, printers) b software c data

Learning outcome
The learner will: 2. Be able to administer user profiles.
Assessment criteria
The learner can: 2.1 make specified changes to user profiles 2.2 specify user profiles to meet individual requirements 2.3 create standard profiles for groups of users 2.4 provide guidance on user profiles to immediate colleagues.

Unit 871 Principles of information security testing

UAN:	**R/505/5815**
Level:	3
Credit value:	12
GLH:	69
Aim:	This unit provides the skills and knowledge necessary to test the information security that has been implemented on a system to establish its effectiveness. Upon successful completion of this unit, learners will be able to plan and carry out the security testing of information systems.

Learning outcome
The learner will: 1. Understand the test process and testing techniques in relation to information security.
Assessment criteria
The learner can: 1.1 describe the impact on organisations and individuals of failures to preserve the confidentiality, integrity and availability of information systems 1.2 explain the role of testing in preserving the confidentiality, integrity and availability of information systems 1.3 explain the impact of information security on the test process 1.4 compare how static and dynamic testing techniques are applied to information security testing 1.5 describe how standard testing techniques are used when testing information security.

Learning outcome
The learner will: 2. Understand the use of common tools for information security testing.
Assessment criteria
The learner can: 2.1 describe how tools can be used to improve efficiency and reliability of information security testing 2.2 explain how to develop plans for information security testing.

Learning outcome
The learner will: 3. Be able to carry out penetration testing.
Assessment criteria
The learner can: 3.1 describe the role and applicability of penetration testing 3.2 describe common penetration testing techniques 3.3 carry out penetration testing according to given specifications.

Unit 872 Principles of secure system development

UAN:	**K/505/5819**
Level:	3
Credit value:	6
GLH:	34
Aim:	This unit provides knowledge and skills required to ensure the secure development of systems. Upon completion of this unit, learners will understand the stages of the systems development life cycle (SDLC) and the associated security requirements.

Learning outcome
The learner will: 1. Understand the role of security in the systems development life cycle (SDLC).
Assessment criteria
The learner can: 1.1 describe common systems development life cycle (SDLC) models 1.2 explain the implications of not including security requirements in each stage of the SDLC 1.3 describe the factors that can influence security requirements including: 1.4 how critical the system is to the organisation 1.5 system requirements for confidentiality, integrity and availability 1.6 applicable regulations and policies 1.7 actual or potential threats in the environment where the system will operate 1.8 identify opportunities for including security requirements in each stage of the SDLC.

Unit 877 Carrying out electronic forensic examinations

Level:	4
Credit value:	12
GLH:	75
Aim:	This unit develops the skills necessary to undertake electronic forensic examinations following an issue involving information, to ensure that evidence is preserved. Upon completion, learners will be able to carry out the actions required to prevent evidence being compromised when investigating an issue involving information security.

Learning outcome
The learner will: 1. Be able to understand what evidence is.
Assessment criteria
The learner can: 1.1 Describe different types of evidence 1.2 Discuss evidence's importance for e-disclosure as part of an investigation 1.3 Demonstrate how to balance the competing demands of business continuity with evidence gathering 1.4 Discuss the role of the expert witness and how it varies from a witness of fact.

Learning outcome
The learner will: 2. Be able to understand what constitutes a crime.
Assessment criteria
The learner can: 2.1 Describe the components of a crime 2.2 Explain the principle of 'burden of proof' 2.3 Describe the importance of 'burden of proof' to disclosure (e-disclosure).

Learning outcome
The learner will: 3. Be able to understand the roles that exist within an investigation.
Assessment criteria
The learner can:

3.1 Describe the different types of investigation that could be undertaken 3.2 Describe the role of the forensic examiner 3.3 Explain the responsibilities and liabilities of a forensic examiner.

Learning outcome
The learner will: 4. Be able to understand the investigation steps.
Assessment criteria
The learner can: 4.1 Describe the investigation steps that are usually undertaken 4.2 Explain how the investigation steps influence the forensic strategy 4.3 Explain the importance of the chain of custody 4.4 Discuss the key principles and methods that would be used in an investigation 4.5 Explain the impact of the key principles and methods may have on an investigation 4.6 Demonstrate recording of actions to withstand the scrutiny from independent third parties.

Learning outcome
The learner will: 5. Be able to understand data storage and digital devices.
Assessment criteria
The learner can: 5.1 Describe where data can be stored and relevant storage devices 5.2 Explain the problems posed for an investigation by the way data is stored 5.3 Explain why operating systems may pose a problem for the investigation 5.4 Discuss the problems posed by various digital devices for a forensic investigator.

Learning outcome
The learner will: 6. Be able to understand different “anti-forensic” techniques.
Assessment criteria
The learner can: 6.1 Describe a range of anti-forensic techniques 6.2 Explain how to identify methods used for anti-forensic purposes 6.3 Discuss what may be done to overcome anti-forensic techniques.

Learning outcome
The learner will: 7. Be able to understand different methods of forensic examination and analysis.
Assessment criteria
The learner can: 7.1 Describe the advantages and disadvantages of live forensics 7.2 Describe the advantages and disadvantages of dead forensics 7.3 Explain when you would use live and dead forensics.

Unit 878 Carrying out information security audits

UAN:	**A/505/5811**
Level:	4
Credit value:	12
GLH:	30
Aim:	This unit provides the knowledge and skills required to plan and undertake information security audits. Upon completion of this unit, learners will be able to plan and undertake security audits that can be used to manage any identified risks.

Learning outcome
The learner will: 1. Be able to prepare for information security audit activities.
Assessment criteria
The learner can: 1.1 interpret given information security audit briefs to identify the information assets and system components to be audited 1.2 identify sources of information relating to the information assets and system components in scope 1.3 develop audit plans, following organisational procedures, which will ensure a thorough assessment of security compliance across the whole scope of the audit 1.4 verify audit scope and plans with relevant persons.

Learning outcome
The learner will: 2. Be able to carry out information security audit activities.
Assessment criteria
The learner can: 2.1 carry out information security audits following organisational procedures 2.2 critically review information and data relating to information assets and system components to assess security compliance 2.3 report any security non-compliance to the relevant persons in line with organisational procedures and timelines 2.4 report on audit activities following organisational procedures 2.5 make justified recommendations for actions to be taken to improve security compliance to relevant persons using media, format and structures which meet the needs of the intended audience.

Unit 879 Carrying out information security forensic examinations

UAN:	**M/505/5806**
Level:	4
Credit value:	9
GLH:	20
Aim:	This unit covers the knowledge and skills necessary to undertake forensic examinations following issues involving information to ensure evidence is preserved. Learners achieving this unit will be able to carry out the activities necessary to prevent evidence being compromised when investigating an issue involving information security.

Learning outcome
The learner will: 1. Be able to carry out information security forensic examinations.
Assessment criteria
The learner can: 1.1 carry out forensic examinations following organisational procedures 1.2 analyse system information for evidence of actual or attempted breaches of security policy or legislation 1.3 report any identified actual or attempted breaches of security to the relevant persons following organisational procedures and timelines 1.4 use security tools to analyse the integrity of software 1.5 take actions to secure information assets and system components subject to actual or attempted breaches of security in line with organisational timelines 1.6 with the authorisation of relevant persons, seize evidence in accordance with legislation and following organisational procedures 1.7 seize evidence, minimising disruption to the organisation and maintaining evidential integrity.

Unit 880 Carrying out information security incident management activities

UAN:	**J/505/5813**
Level:	4
Credit value:	12
GLH:	35
Aim:	This unit covers planning and undertaking activities involved in responding to an incident involving information security. Upon successful completion, learners can undertake activities associated with responding to an incident, making recommendations in line with organisational policies.

Learning outcome
The learner will: 1. Be able to prepare for information security incident management.
Assessment criteria
The learner can: 1.1 interpret given incident investigation briefs to identify the scope of the incidents to be managed 1.2 verify the scope of identified incidents with relevant persons 1.3 evaluate sources of evidence relating to identified incidents.

Learning outcome
The learner will: 2. Be able to manage information security incidents.
Assessment criteria
The learner can: 2.1 obtain evidence relating to identified incidents, following organisational procedures 2.2 critically review evidence to determine appropriate investigative actions 2.3 make justified recommendations for investigative actions to relevant persons using media, format and structures which meet the needs of the intended audience 2.4 report on incident investigation following organisational procedures 2.5 critically evaluate organisational procedures for Incident Investigation.

Unit 881 Carrying out information security risk assessment

UAN:	**A/505/5792**
Level:	4
Credit value:	12
GLH:	40
Aim:	This unit covers the knowledge and skills necessary to plan and undertake an information security risk assessment. Upon completion of the unit, learners will be able to interpret risk assessment briefs and identify the information required to allow them to plan and carry out an effective security risk assessment.

Learning outcome
The learner will: 1. Be able to prepare for information security risk assessments.
Assessment criteria
The learner can: 1.1 interpret given risk assessment briefs to identify the information assets and system components to be assessed 1.2 verify the scope of identified information assets and system components with relevant persons 1.3 evaluate sources of information relating to potential risks that may impact on the security of identified information assets and system components.

Learning outcome
The learner will: 2. Be able to carry out information security risk assessments.
Assessment criteria
The learner can: 2.1 use a range of investigative methods to gather information relating to potential risks that may impact on the security of identified information assets and system components 2.2 record all gathered information in line with organisational requirements 2.3 analyse gathered information to identify risks to the security of identified information assets and system components 2.4 assess identified risks to determine their probability of occurrence and potential impact 2.5 evaluate risks against organisational risk tolerance levels

2.6	report any risks which exceed organisational risk tolerance levels to the relevant persons following organisational procedures and timelines
2.7	formulate actions to mitigate risks
2.8	report the results of risk assessment in line with organisational procedures
2.9	communicate the results and implications of risk assessments to relevant persons using media, format and structures which meet the needs of the intended audience
2.10	evaluate organisational procedures for risk assessment.

Unit 882 Carrying out information security risk management

UAN:	**L/505/5814**
Level:	4
Credit value:	12
GLH:	40
Aim:	This unit enables learners to develop the knowledge and skills necessary to carry out information security risk management. Upon completion of the unit, learners will be able to plan and undertake tasks associated with risk management to mitigate any risks to systems and networks.

Learning outcome
The learner will: 1. Be able to develop information security risk contingency plans.
Assessment criteria
The learner can: 1.1 interpret given risk management briefs to identify the information assets and system components to be covered by the risk contingency plan 1.2 verify the scope of identified information assets and system components with relevant persons 1.3 develop risk contingency plans on a given analysis of the probability and impact of all identified risks 1.4 justify the range of response actions that may be used to mitigate risks 1.5 evaluate risk contingency plans against external standards and legislation 1.6 record information security risk contingency plans in line with organisational requirements.

Learning outcome
The learner will: 2. Be able to manage information security risks.
Assessment criteria
The learner can: 2.1 manage defined response actions to risks which impact the integrity of information assets and system components following organisational procedures and timelines 2.2 report any risks arising for which no response actions have been defined to the relevant persons following organisational procedures and timelines 2.3 report on information security risk management activities following organisational procedures 2.4 communicate the results and implications of risk management activities to relevant persons using media, format and structures which meet the needs of the intended audience 2.5 evaluate organisational procedures for risk management.

Unit 883 Designing and developing event-driven computer programs

UAN:	**J/601/3300**
Level:	4
Credit value:	15
GLH:	90
Aim:	The aim of this unit is to teach the concepts of event-driven programming. In order to do this the learner will learn some of the features of an event-driven environment such as using standard input and output commands and use the integrated development environment effectively. They will have an opportunity to use what they have learnt by modifying an existing program to improve its quality. The learner will test their amended cost against actual and expected outcomes. Lastly the learner will develop design documentation for use in program maintenance as well as end user documentation such as a user guide.

Learning outcome
The learner will: 1. Be able to design event-driven programs to address loosely defined problems.
Assessment criteria
The learner can: 1.1 identify and structure the components and data required to address problems 1.2 select and use pre-defined components, specialising as required 1.3 identify the set of events that invoke behaviour of components and other programme elements 1.4 specify the behaviour of components and other program elements to allow efficient implementation, selecting appropriate data types, data and file structures and algorithms 1.5 record the design using well-established notations.

Learning outcome
The learner will: 2. Be able to produce a working event-driven program which meets the design specification.
Assessment criteria
The learner can: 2.1 make effective use of basic programming language features and programming concepts to implement a program that satisfies the design specification 2.2 make effective use of the features of the programming environment

2.3 make effective use of user interface components in the implementation of the program 2.4 make effective use of a range of debugging tools.

Learning outcome
The learner will: 3. Be able to develop event-driven programs that reflect established programming and software engineering practice.
Assessment criteria
The learner can: 3.1 apply standard naming, layout and comment conventions 3.2 apply appropriate data validation and error handling techniques.

Learning outcome
The learner will: 4. Be able to develop test strategies and apply these to event-driven programs.
Assessment criteria
The learner can: 4.1 develop and apply a test strategy consistent with the design identifying appropriate test data 4.2 apply regression testing consistent with the test strategy 4.3 use appropriate tools to estimate the performance of the program.

Learning outcome
The learner will: 5. Be able to develop design documentation for use in program maintenance and end-user documentation.
Assessment criteria
The learner can: 5.1 record the final state of the program in a form suitable for subsequent maintenance 5.2 provide end-user documentation that meets the user's needs.

Unit 884 Designing and developing object-oriented computer programs

UAN:	**T/601/3308**
Level:	4
Credit value:	15
GLH:	90
Aim:	The aim of this unit is to teach the concepts of designing and developing object-orientated programs. As part this unit, the learner will learn some of the key elements of object-orientated languages such as how to declare file structures and how to use some of the predefined functions. The learner will have an opportunity to use what they have learnt to modify an existing program to improve its quality or write a new program. The learner will test the revised code and record expected and actual results.

Learning outcome
The learner will: 1. Be able to design object-oriented programs to address loosely defined problems.
Assessment criteria
The learner can: 1.1 identify a set of classes and their interrelationships to address the problem 1.2 make effective use of encapsulation, inheritance and polymorphism 1.3 select and reuse pre-existing objects and templates specialising as required 1.4 structure the design so that objects communicate efficiently 1.5 specify the properties and behaviour of classes to allow efficient implementation, selecting appropriate data types, data and file structures and algorithms 1.6 record the design using well-established notations.

Learning outcome
The learner will: 2. Be able to produce a working object-oriented program which meets the design specification.
Assessment criteria
The learner can: 2.1 make effective use of basic programming language features and programming concepts to implement a program that satisfies the design specification 2.2 make effective use of the features of the programming environment 2.3 make effective use of user interface components in the implementation of the program

2.4 make effective use of a range of debugging tools.

Learning outcome
The learner will: 3. Be able to develop object-oriented programs that reflect established programming and software engineering practice.
Assessment criteria
The learner can: 3.1 apply standard naming, layout and comment conventions 3.2 apply appropriate data validation and error handling techniques.

Learning outcome
The learner will: 4. Be able to develop test strategies and apply these to object-oriented programs.
Assessment criteria
The learner can: 4.1 develop and apply a test strategy consistent with the design identifying appropriate test data 4.2 apply regression testing consistent with the test strategy 4.3 use appropriate tools to estimate the performance of the program.

Learning outcome
The learner will: 5. Be able to develop design documentation for use in program maintenance and end-user documentation.
Assessment criteria
The learner can: 5.1 record the final state of the program in a form suitable for subsequent maintenance 5.2 provide end-user documentation that meets the user's needs.

Unit 885 Designing and developing procedural computer programs

UAN:	**T/601/3311**
Level:	4
Credit value:	15
GLH:	90
Aim:	The aim of this unit is to teach the concepts of procedural programming. As part this unit the learner will learn some of the key elements of a procedural language such as how to declare file structures and how to use some of the predefined functions. They will have an opportunity to use what they have learnt by modifying an existing program to improve its quality. They will test the revised code and record expected and actual results. Lastly the learner will develop design documentation for use in program maintenance as well as end user documentation such as a user guide.

Learning outcome
The learner will: 1. Be able to design procedural programs to address loosely defined problems.
Assessment criteria
The learner can: 1.1 identify and structure procedures and functions to address problems 1.2 select and use library functions and procedures 1.3 structure the design with regard to coupling and cohesion 1.4 specify the behaviour of functions and procedures to allow efficient implementation, selecting appropriate data types, data and file structures and algorithms 1.5 record the design using well-established notations.

Learning outcome
The learner will: 2. Be able to produce a working procedural program which meets the design specification.
Assessment criteria
The learner can: 2.1 make effective use of basic programming language features and programming concepts to implement a program that satisfies the design specification 2.2 make effective use of the features of the programming environment

2.3 make effective use of user interface components in the implementation of the program 2.4 make effective use of a range of debugging tools.

Learning outcome
The learner will: 3. Be able to develop procedural programs that reflect established programming and software engineering practice.
Assessment criteria
The learner can: 3.1 apply standard naming, layout and comment conventions 3.2 apply appropriate data validation and error handling techniques.

Learning outcome
The learner will: 4. Be able to develop test strategies and apply these to procedural programs.
Assessment criteria
The learner can: 4.1 develop and apply a test strategy consistent with the design identifying appropriate test data 4.2 apply regression testing consistent with the test strategy 4.3 use appropriate tools to estimate the performance of the program.

Learning outcome
The learner will: 5. Be able to develop design documentation for use in program maintenance and end-user documentation.
Assessment criteria
The learner can: 5.1 record the final state of the program in a form suitable for subsequent maintenance 5.2 provide end-user documentation that meets the user's needs.

Unit 887 Investigating and defining customer requirements for ICT systems

UAN:	**R/602/1772**
Level:	4
Credit value:	15
GLH:	90
Aim:	This unit shows learners how to investigate and define customer requirements for ICT systems. Learners will use different methods of investigation, learn how to record their findings and present them to colleagues. They will also be shown how to analyse information and identify the needs and constraints in meeting the requirements of their customers.

Learning outcome
The learner will: 1. Be able to control the investigation of existing and proposed systems and processes.
Assessment criteria
The learner can: 1.1 select and use the investigative methods which will elicit relevant information about existing and proposed systems and processes 1.2 create the documentation required to record the results of investigations 1.3 ensure that investigative methods are applied correctly, and all relevant information is recorded using standard documentation 1.4 ensure that the confidentiality of customer information is preserved 1.5 provide advice and guidance to colleagues on investigation and analysis of information.

Learning outcome
The learner will: 2. Be able to analyse information to identify needs and constraints.
Assessment criteria
The learner can: 2.1 explain the types of defects and their causes which can arise in information 2.2 describe methods of minimising defects in information 2.3 explain how customer needs and constraints can affect the design of an ICT system 2.4 analyse information to identify customer needs and priorities for: a. data to be stored and processed b. functionality in terms of inputs, processes and outputs c. capacity including numbers of users, throughput, and data storage. 2.5 analyse information to identify customer constraints 2.6 verify that identified needs, priorities and constraints meet customer requirements.

Unit 888 Investigating information security incidents

UAN:	**D/505/5798**
Level:	4
Credit value:	12
GLH:	35
Aim:	This units develops the necessary skills and knowledge to gather and analyse information regarding an information security incident. Learners will be able to interpret information gathered to identify the impact of the incident and make recommendations about the mitigation of risks.

Learning outcome
The learner will: 1. Be able to prepare for information security incident investigations.
Assessment criteria
The learner can: 1.1 interpret given incident investigation briefs to identify the scope of the incidents to be investigated 1.2 verify the scope of identified incidents with relevant persons 1.3 evaluate sources of evidence relating to identified incidents.

Learning outcome
The learner will: 2. Be able to investigate information security incidents.
Assessment criteria
The learner can: 2.1 obtain evidence relating to identified incidents, following organisational procedures 2.2 critically review evidence to determine appropriate investigative actions 2.3 make justified recommendations for investigative actions to relevant persons using media, format and structures which meet the needs of the intended audience 2.4 report on incident investigation following organisational procedures 2.5 critically evaluate organisational procedures for incident investigation.

Unit 889 IT and telecoms system management

UAN:	**M/504/5504**
Level:	4
Credit value:	15
GLH:	90
Aim:	This unit provides the understanding of managing IT & telecoms systems and the skills required. Upon completion of the unit, learners will know how to configure IT & telecoms systems to meet customer requirements and review existing configurations, making recommendations about how these may be optimised.

Learning outcome
The learner will: 1. Understand how to manage systems.
Assessment criteria
The learner can: 1.1 explain how to align system functionality with organisational objectives and customer needs 1.2 explain the types of configurations and asset information associated with systems 1.3 explain the types and applications of system management and monitoring tools.

Learning outcome
The learner will: 2. Be able to review the functionality and management of systems.
Assessment criteria
The learner can: 2.1 evaluate the functionality of systems against organisational objectives and customer needs to identify possible improvements 2.2 evaluate current system configuration and asset information to identify possible enhancements to performance and capacity 2.3 assess current system management and monitoring tools, and their use, suggesting possible improvements 2.4 review, and where necessary update, working procedures for system management 2.5 evaluate the impact of regulatory requirements on system management.

Learning outcome
The learner will: 3. Be able to manage systems.
Assessment criteria
The learner can: 3.1 select and implement configuration options to optimise system performance and capacity 3.2 ensure that changes made to system configurations are effective 3.3 recognise and resolve any system problems arising from configuration changes 3.4 audit records of system configuration and asset information for completeness and accuracy 3.5 evaluate potential risks, including security threats, to systems 3.6 contribute to the development of the organisation's system management strategy.

Unit 890 IT and telecoms system operation

UAN:	**R/504/5513**
Level:	4
Credit value:	15
GLH:	90
Aim:	This unit develops learners' understanding of the architecture used in IT & telecoms systems. Upon successful completion, learners will know how to maintain IT & telecoms systems and review existing configurations, making recommendations about how these may be optimised.

Learning outcome
The learner will: 1. Understand the technical architecture of it or telecom systems.
Assessment criteria
The learner can: 1.1 explain the technical architecture of a system and describe alternative approaches 1.2 explain the contribution to overall system functionality of the main physical and logical components of the system 1.3 explain how system components can be physically and logically interconnected 1.4 describe the external connections of the system and how they are used 1.5 explain the facilities available for controlling and monitoring the operation of the system.

Learning outcome
The learner will: 2. Understand how to specify system operation parameters.
Assessment criteria
The learner can: 2.1 explain how the expected functionality and capacity of the system has been specified 2.2 explain how qualitative and quantitative measures of system operation have been derived from functionality and capacity specifications 2.3 explain how the system can be controlled to optimise performance 2.4 explain how monitoring can be used to measure the qualitative and quantitative operation of the system 2.5 describe the routine maintenance or replenishment required to maintain normal system operation.

Learning outcome
The learner will: 3. Be able to control the operation of systems.
Assessment criteria
The learner can: 3.1 select the control facilities to be used and document how they are to be used to optimise system operation 3.2 select the monitoring facilities to be used and document how they are to be used to identify actual and potential deviations from normal system operation 3.3 define and implement procedures to check the validity of reported deviations from normal system operation 3.4 define and implement procedures to investigate identified and reported deviations to identify required corrective actions 3.5 define the system performance information to be recorded.

Learning outcome
The learner will: 4. Be able to control system maintenance.
Assessment criteria
The learner can: 4.1 define and implement procedures to schedule maintenance and replenishment activities to minimise disruption to system operation 4.2 define and implement procedures to ensure that maintenance activities are carried out safely and in accordance with relevant regulations 4.3 define and implement procedures to ensure that system users are promptly informed of changes to system availability or performance during maintenance activities 4.4 define the maintenance and replenishment information to be recorded.

Unit 891 Testing the security of information systems

UAN:	**A/505/5789**
Level:	4
Credit value:	15
GLH:	60
Aim:	This unit aims to develop the knowledge and skills required to test the information security implemented on a system to establish its effectiveness. Upon completion of this unit, learners will be able to plan and carry out the security testing of information systems using a verity of tools/methods.

Learning outcome
The learner will: 1. Be able to plan security testing.
Assessment criteria
The learner can: 1.1 develop a context driven test approach to systematically test specified parts of a system in order to assess their information security status 1.2 analyse given information assurance requirements to produce information security test acceptance criteria 1.3 develop test scripts and plans to ensure that all information assurance requirements are tested 1.4 prioritise testing activity to target the most significant threats and vulnerabilities first 1.5 select, and where necessary adapt, methods, tools and techniques to conduct penetration testing 1.6 define all required test preparation and conclusion activities.

Learning outcome
The learner will: 2. Be able to carry out security testing.
Assessment criteria
The learner can: 2.1 ensure that all required preparations are implemented, in line with test plans, prior to carrying out tests 2.2 apply test methods, tools and techniques following organisational procedures 2.3 record the results of tests using organisational documentation 2.4 ensure that all required activities have been correctly implemented following the completion of testing in line with test plans 2.5 critically evaluate the results of testing to accurately identify specific vulnerabilities

2.6	prioritise identified vulnerabilities against information assurance requirements
2.7	determine and justify actions to mitigate identified vulnerabilities
2.8	report the results of test activities following organisational procedures
2.9	communicate the results and implications of test activities to relevant persons using media, format and structures which meet the needs of the intended audience
2.10	evaluate organisational procedures for carrying out security testing

Appendix 1 Glossary

Agree	to reach a joint decision (with one or more person(s))
Analyse	to study or examine a topic in detail, in order to discover more about it
Annotation	words/notes written on material (eg photographs or text) usually to personalise or clarify the material
Assessor observation	written evidence produced by the assessor to record what they have observed the learner doing
Attitude	the way a person views something (NB learners do not have to distinguish between skills, qualities and attitudes)
Learner portfolio	see 'portfolio'
Learner statement	information provided by the learner which can be handwritten, typed or presented as a video or audio recording
Choose	select from a number of alternatives
Decide	reach a decision eg by considering options (these options may be suggested by the learner or another person)
Define	say (orally or in writing) what the meaning of something, especially a word, is (eg defining a particular term)
Demonstrate	show how something should be done. This is evidence of performance.
Describe	give details, to say or write what someone or something is like
Evaluate	to judge or calculate the quality, importance, amount or value of something
Explain	to make something clear or easy to understand by describing or giving information about it
Identify	to recognise something (or someone) and say (or prove) what (or who) they are
List	to make a list of at least two items. This could be a written list produced by the learner (eg hand written, using ICT, by highlighting or cutting and pasting from given source materials). Oral evidence could be recorded as an assessor observation, audio recording or a record of questioning.
Outline	give a general explanation or description without detail
Portfolio	a collection of evidence which meets the assessment criteria. This can be paper based and/or stored electronically (ie e-portfolio).
Qualities	distinguishing characteristics or attributes; a feature of personality (NB learners do not have to distinguish between skills, qualities and attitudes)
Range	at least three
Research	find information eg from a variety of oral and/or written sources
Skill	special ability or expertise, often acquired through training (NB learners do not have to distinguish between skills, qualities and attitudes)
State	can be written or oral evidence. Evidence for oral contribution could be an assessor record of questioning.
UAN	Unit accreditation number
Use	to put something such as a tool or skill to a particular purpose
Witness statement	written evidence produced by someone other than the assessor to record what they have observed the learner doing

Appendix 2 Change detail

Version and date	Change detail	Section
1.1 Oct 2012	Amendment to the credit value for unit 208	Structure of the units
2.0 Jan 2013	Missing Units 190 & 191 Added	Structure of the units
2.1 March 2013	Amendment to GLH for unit 214 and corrected unit formatting.	Structure of the units
3.0 October 2013	Missing Unit 360 added.	Structure of the units
3.1 January 2014	Correct GLH and credit value of unit 220	Units
3.2 March 2014	Corrected assessment criteria 2.1 in unit 308 to match Ofqual Register	Units
3.3 March 2014	Corrected UAN number for unit 304	Units
4.0 June 2014	Units 501 – 505 units added	Structure of the units
6.0 December 2015	Units 438-451 and 580 added.	Structure of the units
	Unit 288 – assessment method corrected to Portfolio Unit 384 title corrected Unit 416 title corrected Unit 580 credit value corrected to 14	Units
7.0 February 2017	Unit 4520-416 title corrected	Unit title
8.0 February 2022	Units deleted and added as part of a structural amendment to the qualification. References to e-skills UK removed. Minor amendments to text for clarity.	Units
05 September 2023	Correction of Learning Outcome numbering for Unit 644	Units

About City & Guilds

As the UK's leading vocational education organisation, City & Guilds is leading the talent revolution by inspiring people to unlock their potential and develop their skills. We offer over 500 qualifications across 28 industries through 8500 centres worldwide and award around two million certificates every year. City & Guilds is recognised and respected by employers across the world as a sign of quality and exceptional training.

City & Guilds Group

The City & Guilds Group operates from three major hubs: London (servicing Europe, the Caribbean and Americas), Johannesburg (servicing Africa), and Singapore (servicing Asia, Australia and New Zealand). The Group also includes ILM (management and leadership qualifications), City & Guilds Licence to Practice (land-based qualifications), the Centre for Skills Development (CSD works to improve the policy and practice of vocational education and training worldwide) and Learning Assistant (an online e-portfolio).

Published by City & Guilds, a registered charity established to promote education and training

City & Guilds
Giltspur House
5-6 Giltspur Street
London EC1A 9DE

www.cityandguilds.com