QUALIFICATION HANDBOOK

Level 3 Diploma in Information Security (7550-03)

January 2014 Version 1.3 (September 2016)

City & Guilds

Qualification at a glance

Subject area	**Information Security**
City & Guilds number	7550
Age group approved	16-18, 19+
Entry requirements	n/a
Assessment	By portfolio
Support materials	Centre handbook
Registration and certification	Consult the Walled Garden/Online Catalogue for last dates

Title and level	City & Guilds number	Accreditation number
Level 3 Diploma in Information Security	7550-03	601/1487/3

Version and date	Change detail	Section
1.2 March 2014	Corrected title and UAN of unit 405	**Units**
1.3 September 2016	Unit 415 Added Assessment criteria 2.4 amended in unit 320 Group Statement Amended	**Unit, Structure**

Contents

1 Introduction

This document tells you what you need to do to deliver the qualification:

Area	Description
Who is the qualification for?	It is for learners who work or want to work as information/cyber security personnel, in an assistant role.
What does the qualification cover?	The growth of hacking and phishing across the Internet requires well trained and tested professionals. The Level 3 Diploma in Information Security is designed to provide the knowledge and skills for dealing with cyber security issues and how to work with others to combat them. This is also the main qualification with the Advanced Apprenticeship in Information Security.
Is the qualification part of a framework or initiative?	This qualification is based on the National Occupational Standards and IISP skills Framework.
Who did we develop the qualification with?	It was developed in association with e-Skills UK.
What opportunities for progression are there?	Those who have undertaken an Intermediate Apprenticeship for IT, Web, Software and Telecoms Professionals may wish to progress to this qualification and its Advanced Apprenticeship as an alternative to the Advanced Apprenticeship for IT, Web, Software and Telecoms Professionals. • Level 4 Diploma in Information Security Professional Competence

Structure

To achieve the **Level 3 Diploma in Information Security**, learners must achieve **27** credits from the mandatory units and a minimum of **69** credits from the optional units available. **36** credits must come from Optional groups 1 and 2. **24** of these credits must come from Optional group 1; a further **24** credits must come from Optional group 3. The remaining **9** credits may come from any of the 3 optional groups. Units with the same titles and at different levels are barred against each other.

Unit accreditation number	City & Guilds unit number	Unit title	Credit value	Unit Level	Excluded combination of units (if any)
Mandatory					
Y/500/7183	Unit 101	Health and Safety in ICT	3	1	
D/503/5549	Unit 301	Develop own effectiveness and professionalism	9	3	
K/505/5786	Unit 302	Principles of Information Governance and Assurance	15	3	
Optional group 1					
T/505/5788	Unit 303	Testing the security of Information Systems	12	3	Cannot be taken with unit 402
T/505/5791	Unit 304	Carrying out Information Security Risk Assessment	9	3	Cannot be taken with unit 403
F/505/5793	Unit 305	Investigating Information Security incidents	9	3	Cannot be taken with unit 404
F/505/5812	Unit 306	Carrying out Information Security Incident Management activities	9	3	Cannot be taken with unit 405
R/505/5801	Unit 307	Carrying out Information Security forensic examinations	6	3	Cannot be taken with unit 406

Unit accreditation number	City & Guilds unit number	Unit title	Credit value	Unit Level	Excluded combination of units (if any)
A/505/5808	Unit 308	Carrying out Information Security audits	6	3	Cannot be taken with unit 407
A/505/5789	Unit 402	Testing the security of Information Systems	15	4	Cannot be taken with unit 303
A/505/5792	Unit 403	Carrying out Information Security Risk Assessment	12	4	Cannot be taken with unit 304
D/505/5798	Unit 404	Investigating Information Security incidents	12	4	Cannot be taken with unit 305
J/505/5813	Unit 405	Carrying out Information Security Incident Management activities	12	4	Cannot be taken with unit 306
M/505/5806	Unit 406	Carrying out Information Security forensic examinations	9	4	Cannot be taken with unit 307
A/505/5811	Unit 407	Carrying out Information Security audits	12	4	Cannot be taken with unit 308
	Unit 415	Carrying out electronic forensic examinations	12	4	
Optional group 2					
F/500/7338	Unit 201	ICT System Operation	9	2	Cannot be taken with unit 309, 408
Y/500/7331	Unit 202	System Management	6	2	Cannot be taken with unit 310, 409
T/601/3177	Unit 203	Creating an Event Driven computer program	7	2	Cannot be taken with unit 311, 410
A/601/3181	Unit 204	Creating an Object Oriented computer program	7	2	Cannot be taken with unit 312, 411

Unit accreditation number	City & Guilds unit number	Unit title	Credit value	Unit Level	Excluded combination of units (if any)
L/601/3167	Unit 205	Creating a Procedural computer program	7	2	Cannot be taken with unit 313, 412
H/500/7378	Unit 206	User Profile Administration	6	2	Cannot be taken with unit 315
A/500/7340	Unit 309	System Operation	12	3	Cannot be taken with unit 201, 408
D/500/7332	Unit 310	System Management	12	3	Cannot be taken with unit 202, 409
F/601/3179	Unit 311	Creating an Event Driven computer program	12	3	Cannot be taken with unit 203, 410
L/601/3184	Unit 312	Creating an Object Oriented computer program	12	3	Cannot be taken with unit 204, 411
R/601/3171	Unit 313	Creating a Procedural computer program	12	3	Cannot be taken with unit 205, 412
R/601/3249	Unit 314	Investigating and defining customer requirements for ICT systems	12	3	Cannot be taken with unit 413
K/500/7379	Unit 315	User Profile Administration	9	3	Cannot be taken with unit 206
H/501/4010	Unit 316	Network management and security	14	3	
T/602/2557	Unit 317	Implementing an ICT Systems Security policy	10	3	
R/504/5513	Unit 408	IT & Telecoms System Operation	15	4	Cannot be taken with unit 201, 309
M/504/5504	Unit 409	IT & Telecoms System Management	15	4	Cannot be taken with unit 202, 310

Unit accreditation number	City & Guilds unit number	Unit title	Credit value	Unit Level	Excluded combination of units (if any)
J/601/3300	Unit 410	Designing and developing event-driven computer programs	15	4	Cannot be taken with unit 203, 311
T/601/3308	Unit 411	Designing and developing Object Oriented computer program	15	4	Cannot be taken with unit 204, 312
T/601/3311	Unit 412	Designing and developing Procedural computer program	15	4	Cannot be taken with unit 205, 313
R/602/1772	Unit 413	Investigating and defining customer requirements for IT & Telecoms systems	15	4	Cannot be taken with unit 314
Optional group 3					
L/601/3508	Unit 207	Principles of ICT system and data security	6	2	Cannot be taken with unit 320
A/601/3200	Unit 208	Data Modelling	6	2	Cannot be taken with unit 322
D/601/3206	Unit 209	Data Representation and Manipulation for IT	7	2	Cannot be taken with unit 323
T/601/3289	Unit 210	Networking principles	6	2	Cannot be taken with unit 324
J/601/3295	Unit 211	Telecommunications principles	7	2	Cannot be taken with unit 325
K/505/5819	Unit 318	Principles of secure system development	6	3	
R/505/5815	Unit 319	Principles of Information Security testing	12	3	
R/601/3509	Unit 320	Principles of ICT system and data security	9	3	Cannot be taken with unit 207

Unit accreditation number	City & Guilds unit number	Unit title	Credit value	Unit Level	Excluded combination of units (if any)
T/601/3504	Unit 321	Systems architecture	10	3	
L/601/3203	Unit 322	Data Modelling	9	3	Cannot be taken with unit 208
F/601/3246	Unit 323	Advanced data representation and manipulation for IT	7	3	Cannot be taken with unit 209
J/601/3250	Unit 324	Networking principles	10	3	Cannot be taken with unit 210
D/601/3254	Unit 325	Telecommunications principles	10	3	Cannot be taken with unit 211

2 Centre requirements

Approval

Existing Centres who wish to deliver this qualification will be required to use the **standard** Qualification Approval Process.

Centre who **do not** offer any City & Guilds qualifications will need to gain both centre and qualification approval. Please refer to the *Centre Manual - Supporting Customer Excellence* for further information.

Centre staff should familiarise themselves with the structure, content and assessment requirements of the qualification[s] before designing a course programme.

Resource requirements

Physical resources and site agreements

Centres can use specially designated areas within a centre to assess, for example, user profile administration and Principles units. The equipment, systems and machinery must meet industrial standards and be capable of being used under normal working conditions.

Centre staffing

Staff delivering this qualification must be able to demonstrate that they meet the following occupational expertise requirements. They should:

- be occupationally competent or technically knowledgeable in the areas] for which they are delivering training and/or have experience of providing training. This knowledge must be to the same level as the training being delivered
- have recent relevant experience in the specific area they will be assessing
- have credible experience of providing training.

Centre staff may undertake more than one role, eg tutor and assessor or internal quality assurer, but cannot internally verify their own assessments.

NB: Some employer organisations may require staff to undergo security clearance checks as part of their policy for allowing people on to their premises.

Assessors and Internal Quality Assurer

Assessor/Internal Quality Assurer TAQA qualifications are valued as qualifications for centre staff, but they are not currently a requirement for the qualification.

Staff fulfilling these roles should be trained to a similar standard found within the TAQA qualifications, without being certificated.

Continuing professional development (CPD)

Centres must support their staff to ensure that they have current knowledge of the occupational area, that delivery, mentoring, training, assessment and verification is in line with best practice, and that it takes account of any national or legislative developments.

Age restrictions

City & Guilds cannot accept any registrations for learners under 16 as this qualification is not approved for under 16s.

3 Delivering the qualification

Initial assessment and induction

An initial assessment of each learner should be made before the start of their programme to identify:

- if the learner has any specific training needs,
- support and guidance they may need when working towards their qualification.
- any units they have already completed, or credit they have accumulated which is relevant to the qualification.
- the appropriate type and level of qualification.

We recommend that centres provide an induction programme so the learner fully understands the requirements of the qualification, their responsibilities as a learner, and the responsibilities of the centre. This information can be recorded on a learning contract.

Recording documents

Candidates and centres may decide to use a paper-based or electronic method of recording evidence.

City & Guilds endorses several ePortfolio systems, including our own, **Learning Assistant**, an easy-to-use and secure online tool to support and evidence learners' progress towards achieving qualifications. Further details are available at: **www.cityandguilds.com/eportfolios**.

City & Guilds has developed a set of *Recording forms* including examples of completed forms, for new and existing centres to use as appropriate. *Recording forms* are available on the City & Guilds website.

Although new centres are expected to use these forms, centres may devise or customise alternative forms, which must be approved for use by the qualification consultant, before they are used by candidates and assessors at the centre. Amendable (MS Word) versions of the forms are available on the City & Guilds website.

4 Assessment

Candidates must:

- successfully complete one assignment/portfolio of evidence for each mandatory unit
- successfully complete one assignment/portfolio of evidence for each chosen optional unit or
- successfully complete industry recognised tests for specific units or contribution to holistic evidence as indicated by City & Guilds

Assessment strategy

This qualification has been designed for primary delivery and assessment within a work based setting. Candidates will be assessed within the work place by creating a portfolio of evidence with knowledge units also have the option of being tested using a City & Guilds or Centre Devised assignment.

Recognition of prior learning (RPL)

Recognition of prior learning means using a person's previous experience or qualifications which have already been achieved to contribute to a new qualification.

5 Units

Availability of units

Structure of units

These units each have the following:

- City & Guilds reference number
- unit accreditation number (UAN)
- title
- level
- credit value
- guided learning hours
- learning outcomes which are comprised of a number of assessment criteria

Unit 101 Health and Safety in ICT

UAN:	**Y/500/7183**
Level:	1
Credit value:	3
GLH:	15

Learning outcome
The learner will: 1. Be able to comply with relevant health & safety procedures
Assessment criteria
The learner can: 1.1 identify relevant organisational health & safety procedures 1.2 identify available sources of health & safety information 1.3 demonstrate how relevant health & safety procedures have been followed

Unit 201 ICT System Operation

UAN:	**F/500/7338**
Level:	2
Credit value:	9
GLH:	45

Learning outcome
The learner will: 1. Know the relevant parts of the operating system
Assessment criteria
The learner can: 1.1 describe the relevant parts of operating procedures; a. required service levels (e.g. availability, quality); b. routine maintenance; c. monitoring; d. data integrity (e.g. backups, anti-virus); e. consumables use, storage & disposal; f. health & safety; g. escalation; h. information recording and reporting; i. obtaining work permissions; j. security & confidentiality. 1.2 describe the functionality of relevant parts of the system.

Learning outcome
The learner will: 2. Be able to operate specified parts of the system
Assessment criteria
The learner can: 2.1 operate specified parts of the system a. operating specified system parts following procedures; b. recognising, resolving or escalating system faults; c. gathering and recording specified operational information 2.2 assess and minimize risks related to your own actions such as. a. loss or corruption of data; b. loss of service; c. damage to equipment

Unit 202 System Management

UAN:	**Y/500/7331**
Level:	2
Credit value:	6
GLH:	55

Learning outcome
The learner will: 1. Know how to assist in administering a system
Assessment criteria
The learner can: 1.1 describe how to use specified system configuration facilities. 1.2 explain what ICT asset and configuration information is to be recorded such as: a. physical attributes (e.g. manufacturer, type, revision, serial number, location, value); b. configuration (e.g. physical and logical addresses, options set, connections).

Learning outcome
The learner will: 2. Be able to change system configurations
Assessment criteria
The learner can: 2.1 make specified changes to system configuration; 2.2 gather and record ICT asset and configuration information for specified items.

Unit 203 Creating an event driven computer program

UAN:	**T/601/3177**
Level:	2
Credit value:	7
GLH:	60

Learning outcome
The learner will: 1. Be able to implement software using event driven programming
Assessment criteria
The learner can: 1.1 declare and initialise variable and data structure types and sizes to implement given requirements 1.2 assign properties to screen components 1.3 associate events, including parameter passing, to screen components 1.4 implement event handling using control structures 1.5 declare file structures 1.6 use standard input/output commands to implement design requirements 1.7 use of operators and predefined functions 1.8 use an integrated development environment (IDE)

Learning outcome
The learner will: 2. Be able to refine an event driven program to improve quality
Assessment criteria
The learner can: 2.1 follow an agreed standard for naming, comments and code layout 2.2 implement data validation for inputs 2.3 implement error handling and reporting 2.4 create documentation for the support and maintenance of a computer program

Learning outcome
The learner will: 3. Be able to test the operation of an event driven program
Assessment criteria
The learner can: 3.1 use the debugging facilities available in the ide 3.2 determine expected test results from given test data 3.3 compare actual test results against expected results to identify discrepancies

Unit 204 Creating an object oriented computer program

UAN:	**A/601/3181**
Level:	2
Credit value:	7
GLH:	60

Learning outcome
The learner will: 1. Be able to implement software using object oriented programming
Assessment criteria
The learner can: 1.1 select, declare and initialise variable and data structure types and sizes to meet given requirements 1.2 define relationships between objects 1.3 implement object behaviours using control structures 1.4 declare file structures 1.5 use standard input/output commands 1.6 use operators and predefined functions 1.7 make effective use of an integrated development environment (ide)

Learning outcome
The learner will: 2. Be able to refine an object oriented program to improve quality
Assessment criteria
The learner can: 2.1 follow an agreed standard for naming, comments and code layout 2.2 implement data validation for inputs 2.3 implement opportunities error handling and reporting 2.4 create on-screen help to assist the users of a computer program

Learning outcome
The learner will: 3. Be able to test the operation of an object oriented driven program
Assessment criteria
The learner can: 3.1 use of the debugging facilities available in the ide 3.2 determine expected test results from given test data 3.3 compare actual results against expected results to identify discrepancies

Unit 205 Creating a procedural computer program

UAN:	**L/601/3167**
Level:	2
Credit value:	7
GLH:	60

Learning outcome
The learner will: 1. Be able to implement software using procedural programming
Assessment criteria
The learner can: 1.1 select, declare and initialise variable and data structure types and sizes to meet given requirements 1.2 implement control structures 1.3 declare file structures 1.4 use standard input/output commands 1.5 use operators and predefined functions 1.6 correctly use parameter passing mechanisms

Learning outcome
The learner will: 2. Be able to refine a procedural programme to improve quality
Assessment criteria
The learner can: 2.1 follow an agreed standard for naming, comments and code layout 2.2 implement data validation for inputs 2.3 implement error handling and reporting 2.4 create documentation to assist the users of a computer programme

Learning outcome
The learner will: 3. Be able to test the operation of a procedural programme
Assessment criteria
The learner can:

3.1	use available debugging tools
3.2	determine expected test results from given test data
3.3	compare actual test results against expected results to identify discrepancies

Unit 206 User Profile Administration

UAN:	**H/500/7378**
Level:	2
Credit value:	6
GLH:	55

Learning outcome
The learner will: 1. Know how to assist in the administration of user profiles
Assessment criteria
The learner can: 1.1 describe how to make changes to user profiles such as: a. user identifier (eg. username); b. password and related information (e.g. change frequency); c. allowed system access (e.g. times, locations) d. allowed access to facilities (e.g. data, software)

Learning outcome
The learner will: 2. Be able to assist in the administration of user profiles
Assessment criteria
The learner can: 2.1 make specified changes to user profiles

Unit 207 Principles of ICT system and data security

UAN:	**L/601/3508**
Level:	2
Credit value:	6
GLH:	45

Learning outcome
The learner will: 1. Know the common types of threat to ICT systems and data
Assessment criteria
The learner can: 1.1 identify common types of physical threats to ICT systems and data (hardware damage, loss and theft) 1.2 identify common types of electronic threats to ICT systems and data (e.g. denial of service, data theft or damage, unauthorised use) 1.3 list the security vulnerabilities associated with remote access technologies (including wireless)

Learning outcome
The learner will: 2. Know how to protect ICT systems
Assessment criteria
The learner can: 2.1 identify methods of providing physical access control and security for ICT systems (locks, biometric controls, CCTV, shielding, fire detection and control) 2.2 state methods of providing electronic access control and security for ICT systems (firewalls, virtual networks, secure connection/transfer protocols, secure wireless connection) 2.3 identify common types of malicious code: a. virus b. trojan c. logic bomb d. worm e. spyware 2.4 identify the characteristics of strong passwords

Learning outcome
The learner will: 3. Be able to be aware of the applications of cryptography to ICT systems and data
Assessment criteria
The learner can: 3.1 state how cryptography can be applied to ICT system and data security 3.2 state how public key infrastructure (PKI) operates

Unit 208 Data modelling

UAN:	**A/601/3200**
Level:	2
Credit value:	6
GLH:	45

Learning outcome
The learner will: 1. Know the basic concepts of logical data modelling
Assessment criteria
The learner can: 1.1 identify entities, attributes and relationships 1.2 state the objectives of data normalisation 1.3 state the purpose of keys

Learning outcome
The learner will: 2. Be able to use simple data modelling techniques to create logical data models
Assessment criteria
The learner can: 2.1 identify and name entities, assigning the correct type and size 2.2 identify entity relationships 2.3 use a standard notation to create a logical data model

Unit 209 Data Representation and Manipulation for IT

UAN:	**D/601/3206**
Level:	2
Credit value:	7
GLH:	60

Learning outcome
The learner will: 1. Be able to manipulate real numbers and integers
Assessment criteria
The learner can: 1.1 describe the difference between real numbers and integers 1.2 express numbers in power and scientific notation 1.3 perform arithmetic on numbers in power and scientific notation including multiplication and division of powers 1.4 round real numbers and estimate the resulting error 1.5 describe how real numbers and integers are represented in computer memory

Learning outcome
The learner will: 2. Be able to use co-ordinate systems and vectors, and linear transformations
Assessment criteria
The learner can: 2.1 describe two dimensional co-ordinate systems 2.2 represent simple shapes by finding the co-ordinates of the vertices 2.3 describe vectors 2.4 produce the polar representation of vectors 2.5 offset and scale shapes described by co-ordinates 2.6 convert between linear to polar co-ordinates 2.7 describe co-ordinate systems used in programming output devices

Learning outcome
The learner will: 3. Be able to use simple functions and basic algebraic operations
Assessment criteria
The learner can: 3.1 express simple problems as mathematical equations 3.2 simplify and change the subject of simple equations 3.3 describe the concept of a function 3.4 obtain the equation of a straight line from a graph 3.5 describe the basic properties of a circle and triangle 3.6 apply trigonometric and inverse trigonometric functions

Learning outcome
The learner will: 4. Be able to apply boolean algebra to problem situations
Assessment criteria
The learner can: 4.1 describe how binary states can be used to represent physical systems 4.2 identify and label the inputs and outputs of a binary representation 4.3 produce a truth table corresponding to a binary representation 4.4 express a truth table as a boolean equation 4.5 simplify a boolean equation using algebraic methods

Unit 210 Networking principles

UAN:	**T/601/3289**
Level:	2
Credit value:	6
GLH:	45

Learning outcome
The learner will: 1. Know the OSI model and the TCP/IP suite
Assessment criteria
The learner can: 1.1 identify the function of the OSI model layers 1.2 list the TCP/IP protocols 1.3 list the types of addresses used on networks and why they are used

Learning outcome
The learner will: 2. Know different network topologies and transmission systems
Assessment criteria
The learner can: 2.1 explain logical network topologies as given in the ieee802 standards for LANS and WANS 2.2 identify the following types of network cabling and connectors: a. cat 5 and rj45 b. cat 5e and rj45 c. cat 6 and rj45 d. thin co-axial and BNC connector e. thick co-axial, and AUI transducer with patch cable f. fibre optic cables and connectors 2.3 describe the different types of wireless LAN 2.4 describe the function of the following network devices: a. interface controller b. repeater c. passive, active and intelligent hubs d. bridge e. switch router f. gateway 2.5 explain the 5-4-3 rule of network design

Learning outcome
The learner will: 3. Know the advantages and disadvantages of different types of network
Assessment criteria
The learner can: 3.1 list the properties, security and sharing advantages and disadvantages of a. peer to peer networks b. client server networks 3.2 list the uses and limitations of a null modem connection

Learning outcome
The learner will: 4. Know media access control methods used in local area networks
Assessment criteria
The learner can: 4.1 list the types of media access control methods used in LANS 4.2 explain what is meant by a collision and how network systems deal with them 4.3 explain the difference between a token bus and a token ring and how the token operates in each 4.4 explain the line encoding used in CSMA/CD and CSMA/CA networks 4.5 identify the limitations of CSMA/CA

Unit 211 Telecommunications principles

UAN:	**J/601/3295**
Level:	2
Credit value:	7
GLH:	60

Learning outcome
The learner will: 1. Understand the electromagnetic spectrum as applied to telecommunications
Assessment criteria
The learner can: 1.1 describe the physical properties of electromagnetic radiation and the relationship between frequency and wavelength 1.2 list the principal bands of the electromagnetic spectrum and their associated frequencies and wavelengths 1.3 identify the main telecommunications applications of electromagnetic radiation.

Learning outcome
The learner will: 2. Know the relationship between telecommunication circuits and transmission lines and their effect on a digital signal
Assessment criteria
The learner can: 2.1 identify the circuit properties (resistance, capacitance, inductance and leakance) of alternating current (AC) circuits and describe their effects on transmission lines 2.2 design an equivalent circuit model of a transmission line using the primary line constants 2.3 describe characteristic impedance in transmission lines including open circuit, short circuit and matched termination

Learning outcome
The learner will: 3. Know how binary information is transmitted as a digital signal
Assessment criteria
The learner can: 3.1 describe the properties of digital signals including frequency, mark space ratio and triggered timing 3.2 describe the advantages of digital signals in terms of regeneration, accuracy and recovery 3.3 explain why digital signals need to modulated onto an analogue carrier 3.4 use keying to demonstrate how a digital signal is modulated onto an analogue carrier

Learning outcome
The learner will: 4. Understand how an analogue signal is converted to a digital signal
Assessment criteria
The learner can: 4.1 identify different ways of converting an analogue signal to a digital signal 4.2 describe linear and non-linear forms of encoding 4.3 calculate signal to noise quantisation errors 4.4 explain aliasing in telecommunications terms and how it can be overcome 4.5 explain the use, and limitations, of the nyquist rule in signal sampling

Learning outcome
The learner will: 5. Know how to demonstrate an understanding of signal multiplexing
Assessment criteria
The learner can: 5.1 describe the following methods of signal multiplexing: a. frequency b. synchronous time c. asynchronous time

Unit 301 Develop own effectiveness and professionalism

UAN:	**D/503/5549**
Level:	3
Credit value:	9
GLH:	45

Learning outcome
The learner will: 1. Be able to develop own personal and professional skills
Assessment criteria
The learner can: 1.1 identify own development needs and the activities needed to meet them 1.2 obtain and review feedback from others on performance 1.3 agree personal goals and participate in development activities to meet them

Learning outcome
The learner will: 2. Be able to work as a member of a team to achieve defined goals and implement agreed plans
Assessment criteria
The learner can: 2.1 effectively plan and manage own time 2.2 recognise and respect diversity, individual differences and perspectives 2.3 accept and provide feedback in a constructive and considerate manner 2.4 understand the responsibilities, interests and concerns of colleagues 2.5 identify and reduce obstacles to effective teamwork

Learning outcome
The learner will: 3. Understand what is meant by professional practice
Assessment criteria
The learner can: 3.1 describe the implications, and applicability for it professionals of: a. Data Protection Act b. Computer Misuse Act 3.2 identify the role of professional bodies for it, and the benefits of membership to individuals and organisations 3.3 describe quality management systems and standards for systems development

Learning outcome
The learner will: 4. Understand the ethical and legislative environment relating to it activities
Assessment criteria
The learner can: 4.1 identify the types of conflicts of interest which can arise for it professionals 4.2 describe the impact on an it organisation of legislation covering: a. processing of financial transactions b. health and safety c. privacy, confidentiality and security d. copyright and intellectual property rights

Learning outcome
The learner will: 5. Be able to improve organisational effectiveness
Assessment criteria
The learner can: 5.1 describe the aims and objectives of the organisation 5.2 describe the organisation's brand or image and how it can be promoted 5.3 identify the organisation's structure, roles and responsibilities 5.4 Identify potential improvements to organisational effectiveness

Unit 302 Principles of Information Governance and Assurance

UAN:	**K/505/5786**
Level:	3
Credit value:	15
GLH:	75

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 303 Testing the security of Information Systems

UAN:	**T/505/5788**
Level:	3
Credit value:	12
GLH:	40

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 304 Carrying out Information Security Risk Assessment

UAN:	**T/505/5791**
Level:	3
Credit value:	9
GLH:	30

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 305 Investigating Information Security incidents

UAN:	**F/505/5793**
Level:	3
Credit value:	9
GLH:	23

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 306 Carrying out Information Security Incident Management activities

UAN:	**F/505/5812**
Level:	3
Credit value:	9
GLH:	25

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 307 Carrying out Information Security forensic examinations

UAN:	**R/505/5801**
Level:	3
Credit value:	6
GLH:	10

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 308 Carrying out Information Security audits

UAN:	**A/505/5808**
Level:	3
Credit value:	6
GLH:	10

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 309 System Operation

UAN:	**A/500/7340**
Level:	3
Credit value:	12
GLH:	100

Learning outcome
The learner will: 1. Know how to operate the system
Assessment criteria
The learner can: 1.1 explain the operating procedures that are applicable to the system, such as: a. required service levels (e.g. availability, quality); b. routine maintenance; c. monitoring; d. data integrity (e.g. backups, anti-virus); e. consumables use, storage & disposal; f. health & safety; g. escalation; h. information recording and reporting; i. obtaining work permissions; j. security & confidentiality. 1.2 describe system functionality during normal operation. 1.3 describe the effects of operational activities on system functionality

Learning outcome
The learner will: 2. Be able to operate systems
Assessment criteria
The learner can: 2.1 use and operate the system following appropriate procedures. 2.2 identify system faults and resolve or escalate system faults as appropriate. 2.3 gather and record specified operational information. 2.4 assess and minimise risks such as: a. loss or corruption of data; b. loss of service; c. damage to equipment; d. effects on customer operations

Learning outcome
The learner will: 3. Be able to maintain and implement system operating procedures
Assessment criteria
The learner can: 3.1 provide advice and guidance on system operation to immediate colleagues. 3.2 select the procedures to be followed. 3.3 schedule operational activities to minimise disruption to system functionality. 3.4 collate operational information

Unit 310 System Management

UAN:	**D/500/7332**
Level:	3
Credit value:	12
GLH:	100

Learning outcome
The learner will: 1. Understand how to administer a system
Assessment criteria
The learner can: 1.1 describe how to configure the system. 1.2 describe ICT asset and configuration information applicable to the system such as: a. physical attributes (e.g. manufacturer, type, revision, serial number, location, value); b. configuration (e.g. physical and logical addresses, options set, connections). 1.3 describe how available options for system configuration affect functionality and capacity.

Learning outcome
The learner will: 2. Be able to administer a system and change system configurations
Assessment criteria
The learner can: 2.1 select configuration options to optimise system functionality and capacity. 2.2 make changes to system configuration. 2.3 specify items for which ICT asset and configuration information is to be recorded.

Unit 311 Creating an event driven computer program

UAN:	**F/601/3179**
Level:	3
Credit value:	12
GLH:	90

Learning outcome
The learner will: 1. Be able to 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 screen components to implement design requirements 1.5 implement event handling 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. Be able to 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 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. Be able to 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. Be able to document an event 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 312 Creating an object oriented computer program

UAN:	**L/601/3184**
Level:	3
Credit value:	12
GLH:	90

Learning outcome
The learner will: 1. Be able to 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. Be able to 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. Be able to 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. Be able to 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 313 Creating a procedural computer program

UAN:	**R/601/3171**
Level:	3
Credit value:	12
GLH:	90

Learning outcome
The learner will: 1. Be able to implement a software design using procedural programming
Assessment criteria
The learner can: 1.1 identify the program modules 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 implement control structures to meet the design algorithms 1.4 select and declare file structures to meet design file storage requirements 1.5 select and use standard input/output commands to implement design requirements 1.6 make effective use of operators and predefined functions 1.7 correctly use parameter passing mechanisms

Learning outcome
The learner will: 2. Be able to refine a procedural program to improve quality
Assessment criteria
The learner can: 2.1 use an agreed standard for naming, comments and code layout 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. Be able to test the operation of a procedural program
Assessment criteria
The learner can: 3.1 make effective use of available debugging tools 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. Be able to document a computer program
Assessment criteria
The learner can: 4.1 create documentation to assist the users of a computer program 4.2 create documentation for the support and maintenance of a computer program

Unit 314 Investigating and defining customer requirements for ICT systems

UAN:	**R/601/3249**
Level:	3
Credit value:	12
GLH:	75

Learning outcome
The learner will: 1. Be able to investigate existing systems and processes
Assessment criteria
The learner can: 1.1 use three of the following investigative methods: a. observations b. examination of existing documents, records or software c. questionnaires d. site surveys 1.2 record the results of investigations using standard documentation 1.3 explain the importance of preserving the confidentiality of customer information

Learning outcome
The learner will: 2. Be able to analyse information to identify needs and constraints
Assessment criteria
The learner can: 2.1 describe the type of defect, including inaccuracy, duplication and omission, which can arise in information 2.2 describe the types of customer needs and constraints which can affect the design of an ICT system 2.3 analyse information to identify customer needs 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 2.4 analyse information to identify customer constraints 2.5 record the results of analyses using standard documentation

Unit 315 User Profile Administration

UAN:	**K/500/7379**
Level:	3
Credit value:	9
GLH:	80

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 (e.g. change frequency); c. allowed system access (e.g. times, locations) 1.2 allowed access to facilities (e.g. data, software).. 1.3 describe how to create and edit user and standard profiles 1.4 describe how user profiles affect access to system facilities such as; a. shared resources (e.g. 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 316 Network management and security

UAN:	**H/501/4010**
Level:	3
Credit value:	14
GLH:	95

Learning outcome
The learner will: 1. Know the principles of network design, performance and management.
Assessment criteria
The learner can: 1.1 explain that network performance is reliant upon three basic principles. 1.2 explain how a hierarchical network design can be used to manage network traffic and help to optimise network performance. 1.3 describe the network characteristics of routers, switches and bridges and their potential effects upon network traffic management. 1.4 describe the effect of broadcast traffic on an ip network, broadcast domains and how to manage such traffic. 1.5 describe how the performance of a switched network typically differs from that of one using hubs. 1.6 describe how differing routing protocol characteristics can affect network performance. 1.7 describe how the selection of appropriate routing protocols can be a factor in understanding and managing network traffic on network links. 1.8 explain how different applications are more sensitive to delay and jitter in congested network. 1.9 explain how network congestion affects differing types of network traffic. 1.10 describe at least 2 possible unauthorised networked applications that may cause excess network traffic problems and relate this to acceptable use and security policies within an organisation.

Learning outcome
The learner will: 2. Know the principles of network security
Assessment criteria
The learner can: 2.1 describe how filters and queuing techniques quality of service (QOS) can be applied to network traffic to address congestion issues relating to differing protocol types. 2.2 describe the use of a software network protocol analyser (sniffer) tool to monitor networks and identify problems

Learning outcome
The learner will: 3. Know how to perform network management functions
Assessment criteria
The learner can: 3.1 describe the difference between a network management system (NMS) and operational support system (OSS). 3.2 describe the elements of an NMS/OSS 3.3 explain the function of MIBS as a collection of access points with agents which report to the management station(s). 3.4 identify and describe the operation of network management protocols 3.5 identify examples of network management software (NMS). 3.6 explain that management software (NMS)and operational support systems (OSS) can be used to remotely configure and alter operating parameters of network devices in real time. 3.7 explain the terms mean time between failures (MTBF), mean time to repair (MTTR), up time, down time and useful life cycle. 3.8 explain the terms redundancy, failover and single point of failure in a networking context and the relationship to MTBF and MTTR

Learning outcome
The learner will: 4. Know how to perform network security functions
Assessment criteria
The learner can: 4.1 identify network equipment that can be remotely monitored and managed 4.2 describe and justify at least 3 scenarios where it would be desirable to deploy redundant systems

Unit 317 Implementing an ICT Systems Security policy

UAN:	**T/602/2557**
Level:	3
Credit value:	10
GLH:	60

Learning outcome
The learner will: 1. Be able to analyse and identify ICT system security issues
Assessment criteria
The learner can: 1.1 interpret building, network and system plans and diagrams 1.2 identify vulnerable areas within an ICT system and the different types of security risks in these areas 1.3 suggest the financial impact to the organisation due to ICT system downtime as a result of security issues 1.4 collate and record the data from the analysis and assessment. 1.5 make suggestions for a security policy based upon the conclusions reached

Learning outcome
The learner will: 2. Be able to implement security on email and instant messaging systems
Assessment criteria
The learner can: 2.1 analyse a given network/ ICT system in relation to email and messaging privacy and security requirements 2.2 research current types of potential risk 2.3 research major cost implications of implementing security solutions 2.4 select and justify the choice of email and messaging security solution with respect to functionality, business requirements and budget availability 2.5 identify the issues and considerations surrounding email and messaging privacy with respect to current laws concerning privacy and data protection 2.6 implement basic security protection on an ICT system 2.7 make recommendations for an organisation wide policy with relation to email and messaging systems and document it.

Learning outcome
The learner will: 3. Be able to implement and maintain internet and network security
Assessment criteria
The learner can: 3.1 interpret diagrams and summaries of installed networking equipment in an organisation 3.2 identify potential security threats and risks in network topologies and diagrams 3.3 identify security risks associated with different networking media technologies 3.4 identify, install and configure hardware and software solutions to protect the network and client devices from attack 3.5 take appropriate action to remove unwanted networking protocols on the ICT network 3.6 select appropriate solutions and technologies to back up important data as part of disaster recovery strategies.

Learning outcome
The learner will: 4. Be able to maintain data integrity and system security
Assessment criteria
The learner can: 4.1 make appropriate recommendations for hardware and software to implement secure access to an organisation's networks 4.2 make recommendations to implement an organisation wide password policy 4.3 configure basic networking protocols in a secure manner on a range of different connections to an internet service provider (ISP) or other remote network

Unit 318 Principles of secure system development

UAN:	**K/505/5819**
Level:	3
Credit value:	6
GLH:	34

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 319 Principles of Information Security testing

UAN:	**R/505/5815**
Level:	3
Credit value:	12
GLH:	69

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 320 Principles of ICT system and data security

UAN:	**R/601/3509**
Level:	3
Credit value:	9
GLH:	75

Learning outcome
The learner will: 1. Understand the common types of threat to ICT systems and data
Assessment criteria
The learner can: 1.1 describe common types of physical threats to ICT systems and data (hardware damage, loss and theft) 1.2 describe common types of electronic threats to ICT systems and data (e.g. denial of service, data theft or damage, unauthorised use) 1.3 explain the security vulnerabilities associated with remote access technologies (including wireless)

Learning outcome
The learner will: 2. Understand how to protect ICT systems
Assessment criteria
The learner can: 2.1 describe methods of providing physical access control and security for ICT systems (locks, biometric controls, CCTV, shielding, fire detection and control) 2.2 describe methods of providing electronic access control and security for ICT systems (firewalls, virtual networks, secure connection/transfer protocols, secure wireless connection) 2.3 differentiate the following access control methods: a. mandatory b. discretionary c. role based

2.4 describe the operation of common types of malicious code:
   a. virus
   b. trojan
   c. logic bomb
   d. worm
   e. spyware

2.5 describe the characteristics of strong passwords and methods of attacking password-protected systems

Learning outcome
The learner will: 3. Understand the applications of cryptography to ICT systems and data
Assessment criteria
The learner can: 3.1 describe cryptographic algorithms: a. hashing b. symmetric c. asymmetric 3.2 describe how cryptography can be applied to ICT system and data security in terms of: a. confidentiality b. integrity c. authentication d. non-repudiation e. access control 3.3 explain the operation of public key infrastructure (PKI) 3.4 explain the concepts of the key management and certificate lifecycles

Unit 321 Systems Architecture

UAN:	**T/601/3504**
Level:	3
Credit value:	10
GLH:	80

Learning outcome
The learner will: 1. Understand the representation of information within a computer and the way it is processed
Assessment criteria
The learner can: 1.1 describe how number systems and data representation are used to store information in a computer 1.2 describe the role of input, output and storage devices 1.3 describe the characteristics of C.P.U. components and the operation of the fetch execute cycle 1.4 describe the operation of a peripheral device using correct technical terminology

Learning outcome
The learner will: 2. Be able to make effective use of the operating environment of current computer systems
Assessment criteria
The learner can: 2.1 use and configure operating system interfaces and functions 2.2 explain the role of process management and concurrent processes in computer operating systems 2.3 describe how operating system features can contribute to data and system security

Learning outcome
The learner will: 3. Know the communication process in distributed operating systems and computer networks
Assessment criteria
The learner can:

3.1	outline the function and operation of distributed operating systems
3.2	outline the functions of data communications systems in enabling network and distributed systems

Learning outcome
The learner will: 4. Know distributed applications and transaction processing in mainframe systems
Assessment criteria
The learner can: 4.1 outline the operation and functions of mainframe systems 4.2 outline the evolution of and characteristics of distributed applications 4.3 outline data and process distribution

Unit 322 Data Modelling

UAN:	**L/601/3203**
Level:	3
Credit value:	9
GLH:	75

Learning outcome
The learner will: 1. Understand the concepts of logical data modelling
Assessment criteria
The learner can: 1.1 describe entities and the types of attributes which can be assigned to them 1.2 describe the type of relationships which can exist between entities 1.3 explain the objectives of data normalisation and describe the third normal form (3nf) 1.4 explain the purpose of keys 1.5 describe an application where un-normalized or de-normalised data may be used 1.6 describe the types of standard notation which can be used to represent data sets as logical data models

Learning outcome
The learner will: 2. Be able to use data modelling techniques to create logical data models
Assessment criteria
The learner can: 2.1 identify and name entities, assigning the correct attributes 2.2 identify and represent entity relationships, assigning the correct type 2.3 normalise a data set to third normal form (3nf)

Learning outcome
The learner will: 3. Be able to use data modelling techniques to refine logical data models
Assessment criteria
The learner can:

3.1	identify entities which will be accessed for enquiry and/or update
3.2	identify access sequences and triggers
3.3	create access rules/methods
3.4	use a standard notation to describe the logical data model of a normalised data set

Unit 323 Advanced data representation and manipulation for IT

UAN:	**F/601/3246**
Level:	3
Credit value:	7
GLH:	60

Learning outcome
The learner will: 1. Be able to apply matrix methods
Assessment criteria
The learner can: 1.1 explain matrices as a method of representing ordered data and their relationship with computer program variable arrays 1.2 use index notation to reference the cells of a matrix 1.3 perform add, subtract and scalar multiplication operations on a matrix 1.4 multiply two matrices 1.5 find: a. the inverse of a matrix by elementary row operations b. the transpose of a matrix 1.6 apply matrix techniques to a range of applications including: a. solving simultaneous linear equations b. vector transformation and rotation c. maps and graphs

Learning outcome
The learner will: 2. Be able to apply series, probability and recursions
Assessment criteria
The learner can: 2.1 give a functional expression for a series 2.2 express a series recursively 2.3 find the sum of a series 2.4 express probabilities as percentages, fractions and decimals 2.5 apply series, probability and recursion techniques to develop a solution to a range of problems

Learning outcome
The learner will: 3. Be able to apply graph theory
Assessment criteria
The learner can: 3.1 describe the components of a graph and their properties 3.2 explain the characteristics of undirected, directed and mixed graphs 3.3 represent a set of connected objects as a graph 3.4 describe the type of problem which can be modelled by a weighted graph

Unit 324 Networking principles

UAN:	**J/601/3250**
Level:	3
Credit value:	10
GLH:	75

Learning outcome
The learner will: 1. Understand physical and logical topologies and systems
Assessment criteria
The learner can: 1.1 describe common physical network topologies 1.2 explain the difference between logical and physical network topologies 1.3 describe the network topologies and hardware and software components used to implement common data communication systems 1.4 identify common a. cable types and properties b. connector types c. wiring standards d. wireless standards

Learning outcome
The learner will: 2. Understand the open system interconnection (OSI) model
Assessment criteria
The learner can: 2.1 describe the OSI model and how its layers relate to each other 2.2 explain the function of each layer of the OSI model 2.3 describe the key features, protocols and standards of each OSI layer

Learning outcome
The learner will: 3. Understand the internet protocol suite (TCP/IP)
Assessment criteria
The learner can: 3.1 describe the internet protocol suite (TCP/IP) and the function of its four layers 3.2 describe the key features, protocols and standards of each TCP/IP layer 3.3 explain how TCP/IP relates to the OSI model

Unit 325 Telecommunications principles

UAN:	**D/601/3254**
Level:	3
Credit value:	10
GLH:	80

Learning outcome
The learner will: 1. Understand the principals of alternating current (ac) circuits
Assessment criteria
The learner can: 1.1 explain a. reactance in circuits b. impedance in terms of resistive and reactive components 1.2 describe the characteristics of series and parallel resonant circuits 1.3 calculate the resonant frequency of a circuit

Learning outcome
The learner will: 2. Understand the effects of line impairments on a transmitted signal
Assessment criteria
The learner can: 2.1 explain; a. decibel (db) as a unit of loss b. dbm as a unit of power 2.2 define signal-to-noise ratio as applied to transmission lines 2.3 calculate using dbs and dbms the a. total loss of a system from individual losses b. total loss of a system from input and output signal levels c. output signal level from total loss and input signal level d. signal-to-noise ratio

Learning outcome
The learner will: 3. Be able to apply the characteristics of transmission lines
Assessment criteria
The learner can: 3.1 explain the effect of the primary line constants r, g, l & c on the characteristic impedance of transmission lines 3.2 define the concept of angular frequency as applied to transmission lines 3.3 calculate, using the primary line constants, the characteristic impedance of: a. finite and infinite line lengths b. a parallel pair of wires c. co-axial cable 3.4 produce an equivalent circuit model of a transmission line in terms of resistance, capacitance and inductance 3.5 calculate the bandwidth of a transmission line in terms of frequency between half power points

Learning outcome
The learner will: 4. Understand the transmission of digital signals over transmission media
Assessment criteria
The learner can: 4.1 demonstrate the following representations of binary information and explain the advantages of each type a. non-return to zero (nrz) digital encoding from given values b. return to zero (rtz) digital encoding from given values c. bi-phase digital encoding (manchester) from given values d. bi-phase digital encoding (differential manchester) from given values 4.2 explain the concepts of bit rate and bit error rate (ber) 4.3 explain digital signal impairments in terms of a. delay b. jitter c. binary errors 4.4 demonstrate the effects of delay, limited bandwidth and jitter on the extraction of binary information from a digital signal

Learning outcome
The learner will: 5. Understand the process of modulating an analogue carrier frequency using digital signals
Assessment criteria
The learner can: 5.1 explain the following methods of digital modulation using analogue

frequency carriers:

a. amplitude shift keying (ask & ook)
b. frequency shift keying (fsk)
c. phase shift keying (psk)
d. bi-polar shift keying (bpsk)
e. quadra-phase shift keying (qpsk)
f. quadrature amplitude shift keying (qam)

5.2 describe the purpose of, and produce constellation diagrams
5.3 calculate the practical channel capacity using:
   a. shannon-hartley formula ?log2(s/n+1)
   b. shannon formula 2?log2(n)
5.4 explain the need for filters and their effect on digitally modulated signals
5.5 calculate the baud rate of a given link states using given values

Learning outcome
The learner will: 6. Understand the process of multiplexing digital and analogue signals over transmission media
Assessment criteria
The learner can: 6.1 explain the following type of multiplexing: a. frequency division b. synchronous time division c. asynchronous time division d. digital time division e. code division f. wavelength (coarse and dense) division

Unit 402 Testing the security of Information Systems

UAN:	**A/505/5789**
Level:	4
Credit value:	15
GLH:	60

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

Unit 403 Carrying out Information Security Risk Assessment

UAN:	**A/505/5792**
Level:	4
Credit value:	12
GLH:	40

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 404 Investigating Information Security incidents

UAN:	**D/505/5798**
Level:	4
Credit value:	12
GLH:	35

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 405 Carrying out Information Security Incident Management activities

UAN:	**J/505/5813**
Level:	4
Credit value:	12
GLH:	35

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 406 Carrying out Information Security forensic examinations

UAN:	**M/505/5806**
Level:	4
Credit value:	9
GLH:	20

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 407 Carrying out Information Security audits

UAN:	**A/505/5811**
Level:	4
Credit value:	12
GLH:	30

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 408 IT & Telecoms System Operation

UAN:	**R/504/5513**
Level:	4
Credit value:	15
GLH:	90

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 409 IT & Telecoms System Management

UAN:	**M/504/5504**
Level:	4
Credit value:	15
GLH:	90

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 configuration 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 410 Designing and developing event-driven computer programs

UAN:	**J/601/3300**
Level:	4
Credit value:	15
GLH:	90

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 411 Designing and developing object-oriented computer programs

UAN:	**T/601/3308**
Level:	4
Credit value:	15
GLH:	90

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 412 Designing and developing procedural computer programs

UAN:	**T/601/3311**
Level:	4
Credit value:	15
GLH:	90

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 413 Investigating and Defining Customer Requirements for ICT Systems

UAN:	**R/602/1772**
Level:	4
Credit value:	15
GLH:	90

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 defect, 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 415 Carrying out electronic forensic examinations

Level:	4
Credit value:	12
GLH:	75

Learning outcome
The learner will: 1. Be able to understand what is evidence
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 the where 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

Appendix 1 Sources of general information

The following documents contain essential information for centres delivering City & Guilds qualifications. They should be referred to in conjunction with this handbook. To download the documents and to find other useful documents, go to the **Centres and Training Providers homepage** on **www.cityandguilds.com**.

Centre Manual - Supporting Customer Excellence contains detailed information about the processes which must be followed and requirements which must be met for a centre to achieve 'approved centre' status, or to offer a particular qualification, as well as updates and good practice exemplars for City & Guilds assessment and policy issues. Specifically, the document includes sections on:

- The centre and qualification approval process
- Assessment, internal quality assurance and examination roles at the centre
- Registration and certification of candidates
- Non-compliance
- Complaints and appeals
- Equal opportunities
- Data protection
- Management systems
- Maintaining records
- Assessment
- Internal quality assurance
- External quality assurance.

Our Quality Assurance Requirements encompasses all of the relevant requirements of key regulatory documents such as:

- Regulatory Arrangements for the Qualifications and Credit Framework (2008)
- SQA Awarding Body Criteria (2007)
- NVQ Code of Practice (2006)

and sets out the criteria that centres should adhere to pre and post centre and qualification approval.

Access to Assessment & Qualifications provides full details of the arrangements that may be made to facilitate access to assessments and qualifications for candidates who are eligible for adjustments in assessment.

The **centre homepage** section of the City & Guilds website also contains useful information on such things as:

- **Walled Garden:** how to register and certificate candidates on line
- **Qualifications and Credit Framework (QCF)**: general guidance about the QCF and how qualifications will change, as well as information on the IT systems needed and FAQs
- **Events**: dates and information on the latest Centre events
- **Online assessment**: how to register for e-assessments.

Useful contacts

UK learners **General qualification information**	**E: learnersupport@cityandguilds.com**
International learners General qualification information	E: **intcg@cityandguilds.com**
Centres Exam entries, Certificates, Registrations/enrolment, Invoices, Missing or late exam materials, Nominal roll reports, Results	E: **centresupport@cityandguilds.com**
Single subject qualifications Exam entries, Results, Certification, Missing or late exam materials, Incorrect exam papers, Forms request (BB, results entry), Exam date and time change	E: **singlesubjects@cityandguilds.com**
International awards Results, Entries, Enrolments, Invoices, Missing or late exam materials, Nominal roll reports	E: **intops@cityandguilds.com**
Walled Garden Re-issue of password or username, Technical problems, Entries, Results, e-assessment, Navigation, User/menu option, Problems	E: **walledgarden@cityandguilds.com**
Employer Employer solutions, Mapping, Accreditation, Development Skills, Consultancy	E: **business@cityandguilds.com**
Publications Logbooks, Centre documents, Forms, Free literature	

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 is a leader in global skills development. Our purpose is to help people and organisations to develop their skills for personal and economic growth. Made up of City & Guilds, City & Guilds Kineo, The Oxford Group and ILM, we work with education providers, businesses and governments in over 100 countries.

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

City & Guilds
1 Giltspur Street
London EC1A 9DD
F +44 (0)20 7294 2413
www.cityandguilds.com