Level 4 Diploma in Information Security Professional Competence (7550-04)

January 2014 Version 1.3 (July 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 4 Diploma in Information Security Professional Competence	7550-04	601/1789/8

Version and date	Change detail	Section
1.2 March 2014	Corrected unit number – 405 to 404	**Structure, Units**
1.3 July 2016	Unit 415 Added Group Statement Amended	**Structure, Units**

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, or for those moving from other areas of ICT to take on the testing and risk assessment of information security.
What does the qualification cover?	The growth of hacking and phishing across the Internet requires well trained and tested professionals. The Level 4 Diploma in Information Security Professional Competence is designed to provide the knowledge and skills for dealing with cyber security issues, how to work with others to combat them and take on the testing and risk assessment of 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.

Structure

To achieve the **Level 4 Diploma in Information Security Professional Competence**, learners must achieve **15** credits from the mandatory units and a minimum of **63** credits from the optional units available. **36** of these credits must come from Optional group 1

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	
K/601/3502	Unit 401	Develop own effectiveness and professionalism	12	4	
Optional group 1					
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
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
L/505/5814	Unit 414	Carrying out Information Security Risk Management	12	4	
	Unit 415	Carrying out electronic forensic examinations	12	4	

City & Guilds Level 4 Diploma in Information Security Professional Competence (7550-04)

Optional group 2

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	
R/505/5801	Unit 307	Carrying out Information Security forensic examinations	6	3	Cannot be taken with unit 406
A/505/5808	Unit 308	Carrying out Information Security audits	6	3	Cannot be taken with unit 407
A/500/7340	Unit 309	System Operation	12	3	Cannot be taken with unit 408
D/500/7332	Unit 310	System Management	12	3	Cannot be taken with unit 409
F/601/3179	Unit 311	Creating an Event Driven computer program	12	3	Cannot be taken with unit 410
L/601/3184	Unit 312	Creating an Object Oriented computer program	12	3	Cannot be taken with unit 411
R/601/3171	Unit 313	Creating a Procedural computer program	12	3	Cannot be taken with unit 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	

R/504/5513	Unit 408	IT & Telecoms System Operation	15	4	Cannot be taken with unit 309
M/504/5504	Unit 409	IT & Telecoms System management	15	4	Cannot be taken with unit 310
J/601/3300	Unit 410	Designing and developing event-driven computer programs	15	4	Cannot be taken with unit 311
T/601/3308	Unit 411	Designing and developing object-oriented computer programs	15	4	Cannot be taken with unit 312
T/601/3311	Unit 412	Designing and developing procedural computer programs	15	4	Cannot be taken with unit 313
R/602/1772	Unit 413	Investigating and Defining Customer Requirements for ICT Systems	15	4	Cannot be taken with unit 314

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

This is a work based competency qualification and it is expected that the employer will provide access to the relevant tools and equipment required by a candidate to allow the to demonstrate their capabilities in order to achieve the units undertaken.

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 a portfolio of evidence for each 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 delivery and assessment within a work based setting. Candidates will be assessed within the work place by creating a portfolio of evidence.

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 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

City & Guilds Level 4 Diploma in Information Security Professional Competence (7550-04)

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

City & Guilds Level 4 Diploma in Information Security Professional Competence (7550-04)

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)
d. allowed access to facilities (e.g. data, software)
1.2 describe how to create and edit user and standard profiles
1.3 describe how user profiles affect access to system facilities such as;
a. shared resources (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 401 Develop own effectiveness and professionalism

UAN:	K/601/3502
Level:	4
Credit value:	12
GLH:	60

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 interpret feedback from others on performance
1.3 set and agree personal goals and participate in development activities to meet them
1.4 manage own personal/professional development in order to achieve career and personal goals.
1.5 reflect critically on own learning

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 and others 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 understand the role of the individual and teams in an IT organisation
2.6 identify and resolve obstacles to effective teamwork

Learning outcome

The learner will:
3. Understand what is meant by professional practice
Assessment criteria
The learner can:
3.1 interpret the implications, and applicability for IT professionals of:
a. Data Protection Act
b. Computer Misuse Act
3.2 describe the role of professional bodies for IT, and the benefits of membership to individuals and organisations
3.3 explain the importance of 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 describe the types of conflicts of interest which can arise for IT professionals
4.2 evaluate 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 interpret the aims and objectives of the organisation
5.2 describe the organisation's brand or image and how it can be promoted
5.3 describe the organisation's structure, roles and responsibilities
5.4 identify and evaluate potential improvements to organisational effectiveness

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 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

City & Guilds Level 4 Diploma in Information Security Professional Competence (7550-04)

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

City & Guilds Level 4 Diploma in Information Security Professional Competence (7550-04)

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 414 Carrying out Information Security Risk Management

UAN:	L/505/5814
Level:	4
Credit value:	12
GLH:	40

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

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

activities to relevant persons using media, format and structures which meet the needs of the intended audience

2.5 evaluate organisational procedures for risk management

Unit 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.

City & Guilds
Believe you can

www.cityandguilds.com

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	

Every effort has been made to ensure that the information contained in this publication is true and correct at the time of going to press. However, City & Guilds' products and services are subject to continuous development and improvement and the right is reserved to change products and services from time to time. City & Guilds cannot accept liability for loss or damage arising from the use of information in this publication.

If you have a complaint, or any suggestions for improvement about any of the services that we provide, email: feedbackandcomplaints@cityandguilds.com