Pearson BTEC Level 4 Diploma in Information Security Professional Competence (QCF)

Specification

Competence-based qualification

First registration August 2014

Edexcel, BTEC and LCCI qualifications

Edexcel, BTEC and LCCI qualifications are awarded by Pearson, the UK's largest awarding body offering academic and vocational qualifications that are globally recognised and benchmarked. For further information, please visit our qualification websites at www.edexcel.com, www.btec.co.uk or www.lcci.org.uk. Alternatively, you can get in touch with us using the details on our contact us page at www.edexcel.com/contactus

About Pearson

Pearson is the world's leading learning company, with 40,000 employees in more than 70 countries working to help people of all ages to make measurable progress in their lives through learning. We put the learner at the centre of everything we do, because wherever learning flourishes, so do people. Find out more about how we can help you and your learners at: www.pearson.com/uk

References to third party material made in this specification are made in good faith. Pearson does not endorse, approve or accept responsibility for the content of materials, which may be subject to change, or any opinions expressed therein. (Material may include textbooks, journals, magazines and other publications and websites.)

All information in this specification is correct at time of publication.

Authorised by Dave Evans
Prepared by Maria Adu

ISBN 978 1 446 9 11877

Contents

Purpose of this specification

The purpose of a specification as defined by Ofqual is to set out:

- the qualification's objective
- any other qualification that a learner must have completed before taking the qualification
- any prior knowledge, skills or understanding that the learner is required to have before taking the qualification
- units that a learner must have completed before the qualification will be awarded and any optional routes
- any other requirements that a learner must have satisfied before they will be assessed or before the qualification will be awarded
- the knowledge, skills and understanding that will be assessed as part of the qualification (giving a clear indication of their coverage and depth)
- the method of any assessment and any associated requirements relating to it
- the criteria against which the learner's level of attainment will be measured (such as assessment criteria)
- any specimen materials
- any specified levels of attainment
- the Apprenticeship Framework in which the qualification is included, where appropriate.

1 Introducing Pearson BTEC Competence-based qualifications

What are Competence-based qualifications?

Competence-based qualifications reflect the skills and knowledge needed to do a job effectively. They are work-based qualifications that give learners the opportunity to demonstrate their competence in the area of work or job role to which the qualification relates.

Competence-based qualifications are outcomes-based with no fixed learning programme, allowing flexibility in their delivery to meet the individual learner's needs. The qualifications are based on the National Occupational Standards (NOS) for the sector, which define what employees, or potential employees, must be able to do and know, and how well they should undertake work tasks and work roles.

Most Competence-based qualifications form the competence component of Apprenticeship Frameworks. They are suitable for those in employment or those who are studying at college and have a part-time job or access to a substantial work placement.

Most learners will work towards their qualification in the workplace or in settings that replicate the working environment. Colleges, training centres and/or employers can offer these qualifications provided they have access to appropriate physical and human resources.

There are three sizes of Competence-based qualification in the QCF:

- Award (1 to 12 credits)
- Certificate (13 to 36 credits)
- Diploma (37 credits and above).

Every unit and qualification in the QCF has a credit value.

The credit value of a unit specifies the number of credits that will be awarded to a learner who has met the learning outcomes of the unit.

The credit value of a unit is based on:

- one credit for those learning outcomes achievable in 10 hours of learning
- learning time – defined as the time taken by learners at the level of the unit, on average, to complete the learning outcomes of the unit to the standard determined by the assessment criteria.

2 Qualification summary and key information

Qualification title	Pearson BTEC Level 4 Diploma in Information Security Professional Competence(QCF)
QCF Qualification Number (QN)	601/3783/6
Qualification framework	Qualifications and Credit Framework (QCF)
Accreditation start date	August 2014
Certification end date	December 2017
Approved age ranges	16–18 19+ Please note that sector-specific requirements or regulations may prevent learners of a particular age from embarking on this qualification.
Credit value	78
Assessment	Portfolio of Evidence (internal assessment)
Guided learning hours	325–395
Grading information	The qualification and units are at Pass grade
Entry requirements	No prior knowledge, understanding, skills or qualifications are required before learners register for this qualification. However, centres must follow the Pearson Access and Recruitment policy (see *Section 9, Access and recruitment*).

QCF qualification number and qualification title

Centres will need to use the QCF Qualification Number (QN) when they seek public funding for their learners. Every unit in a qualification has a QCF unit reference number (URN).

The qualification title, unit titles and QN are given on each learner's final certificate. You should tell your learners this when your centre recruits them and registers them with us. There is more information about certification in our *UK Information Manual,* available on our website at:
www.edexcel.com/iwantto/Pages/uk-information-manual

Qualification objectives

The Pearson BTEC Level 4 Diploma in Information Security Professional Competence (QCF) is for learners who work in, or want to work in the information security sector.

It gives learners the opportunity to:

- demonstrate competence in relevant job roles within the information security sector
- develop knowledge and skills related to the specified job roles in the information security sector
- have existing skills recognised
- achieve a nationally recognised Level 4 qualification
- personally develop and engage in learning.

Relationship with previous qualifications

This is a new qualification.

Apprenticeships

E-skills UK includes the Pearson BTEC Level 4 Diploma in Information Security Professional Competence (QCF) as the competence component for the Higher Apprenticeship in Information Security.

Progression opportunities

Learners who have achieved the Pearson BTEC Level 4 Diploma in Information Security Professional Competence (QCF) may progress to the Pearson BTEC Level 5 HND Diploma in Computing and Systems Development (QCF).

Industry support and recognition

This qualification is supported by e-skills UK, the Sector Skills Council for Information Technology.

Relationship with National Occupational Standards

This qualification is based on the e-skills UK National Occupational Standards (NOS) and the IISP (Information Security and Information Assurance Professionals) skills framework in Information Technology.

3 Qualification structure

Pearson BTEC Level 4 Diploma in Information Security Professional Competence (QCF)

The learner will need to meet the requirements outlined in the table below before the qualification can be awarded.

Minimum number of credits that must be achieved	78
Minimum number of credits that must be achieved at Level 4	48
Number of mandatory credits that must be achieved	15
Number of optional credits that must be achieved from Option Group 1	36
The remaining 27 credits may be achieved from: a combination of Option Group 1 and Option Group 2 OR Option Group 2 only	27

Unit	Unit reference number	Mandatory units All 15 credits MUST be achieved from this group	Level	Credit	Guided learning hours
101	Y/500/7183	Health and Safety in ICT	1	3	15
401	K/601/3502	Develop own Effectiveness and Professionalism	4	12	60
Unit	**Unit reference number**	**Option Group 1 units A minimum of 36 credits MUST be achieved from this group**	**Level**	**Credit**	**Guided learning hours**
TS – Testing Security No more than one unit to be completed from this section					
303	T/505/5788	Testing the Security of Information Systems	3	12	40
403	A/505/5789	Testing the Security of Information Systems	4	15	60
RA – Risk Assessment No more than one unit to be completed from this section					
304	T/505/5791	Carrying Out Information Security Risk Assessment	3	9	30
404	A/505/5792	Carrying Out Information Security Risk Assessment	4	12	40

Unit	Unit reference number	Option Group 1 units A minimum of 36 credits MUST be achieved from this group	Level	Credit	Guided learning hours
II – Investigating Information Security Incidents No more than one unit to be completed from this section					
305	F/505/5793	Investigating Information Security Incidents	3	9	23
405	D/505/5798	Investigating Information Security Incidents	4	12	35
FE – Forensic Examinations No more than one unit to be completed from this section					
307	R/505/580	Carrying Out Information Security Forensic Examinations	3	6	10
407	M/505/5806	Carrying Out Information Security Forensic Examinations	4	9	20
SA – Security Audits No more than one unit to be completed from this section					
308	A/505/580	Carrying Out Information Security Audits	3	6	10
408	A/505/5811	Carrying Out Information Security Audits	4	12	30
RM – Risk Management This single unit may be attempted					
415	L/505/5814	Carrying Out Information Security Risk Management	4	12	40
Unit	**Unit reference number**	**Option Group 2 units. A maximum of 27 credits may be taken from this group.**	**Level**	**Credit**	**Guided learning hours**
MA – Management Activities This single unit may be attempted					
306	F/505/5812	Carrying Out Information Security Incident Management Activities	3	9	25
SO – System Operation No more than one unit to be completed from this section					
309	A/500/7340	System Operation	3	12	100
409	R/504/5513	IT and Telecoms System Operation	4	15	90
SM – System Management No more than one unit to be completed from this section					

Unit	Unit reference number	Option Group 2 units. A maximum of 27 credits may be taken from this group.	Level	Credit	Guided learning hours
310	D/500/7332	System Management	3	12	100
410	M/504/5504	IT and Telecoms System Management	4	15	90
ED – Event-Driven Computer Program No more than one unit to be completed from this section					
311	F/601/3179	Creating an Event-Driven Computer Program	3	12	90
411	J/601/3300	Designing and Developing Event-Driven Computer Program	4	15	90
OO – Object-Oriented Computer Program No more than one unit to be completed from this section					
312	L/601/3184	Creating an Object-Oriented Computer Program	3	12	90
412	T/601/3308	Designing and Developing Object-Oriented Computer Program	4	15	90
CP – Creating a Procedural Computer Program No more than one unit to be completed from this section					
313	R/601/3171	Creating a Procedural Computer Program	3	12	90
413	T/601/3311	Designing and Developing Procedural Computer Program	4	15	90
ID – Investigating and Defining No more than one unit to be completed from this section					
314	R/601/3249	Investigating and Defining Customer Requirements for ICT Systems	3	12	75
414	R/602/1772	Investigating and Defining Customer Requirements for ICT Systems	4	15	90
UP – User Profile Administration This single unit may be attempted					
315	K/500/7379	User Profile Administration	3	9	80

4 Assessment

This qualification is assessed through an externally verified Portfolio of Evidence that consists of evidence gathered during the course of the learner's work.

To achieve a Pass for the full qualification, the learner must achieve all the required units in the stated qualification structure. Each unit has specified learning outcomes and assessment criteria. To pass each unit the learner must:

- achieve **all** the specified learning outcomes
- satisfy **all** the assessment criteria by providing sufficient and valid evidence for each criterion
- prove that the evidence is their own.

The learner must have an assessment record that identifies the assessment criteria that have been met, and it should be cross-referenced to the evidence provided. The assessment record should include details of the type of evidence and the date of assessment. The unit specification or suitable centre documentation can be used to form an assessment record.

It is important that the evidence provided to meet the assessment criteria of the unit and learning outcomes is:

Valid	relevant to the standards for which competence is claimed
Authentic	produced by the learner
Current	sufficiently recent to create confidence that the same skill, understanding or knowledge persist at the time of the claim
Reliable	indicates that the learner can consistently perform at this level
Sufficient	fully meets the requirements of the standards.

Learners can provide evidence of occupational competence from:

- **current practice** where evidence is generated from a current job role
- a **programme of development** where evidence comes from assessment opportunities built into a learning programme.
- the **Recognition of Prior Learning (RPL)** where a learner can demonstrate that they can meet the assessment criteria within a unit through knowledge, understanding or skills they already possess without undertaking a course of development. They must submit sufficient, reliable, authentic and valid evidence for assessment. Evidence submitted based on RPL should provide confidence that the same level of skill/understanding/knowledge exists at the time of claim as existed at the time the evidence was produced. RPL is acceptable for accrediting a unit, several units, or a whole qualification.
- Further guidance is available in the policy document *Recognition of Prior Learning Policy and process*, available on our website: www.edexce.com/polices
- a **combination** of these.

Assessment requirements

Learners must provide evidence according to the requirements stated in the unit.

Types of evidence

To achieve a unit, the learner must gather evidence that shows that they have met the required standard specified in the assessment criteria. The evidence for this qualification can take a variety of forms as indicated below:

- direct observation of the learner's performance by their assessor (O)
- outcomes from oral or written questioning (Q&A)
- products of the learner's work (P)
- personal statements and/or reflective accounts (RA)
- outcomes from simulation (S)
- professional discussion (PD)
- assignment, project/case studies (A)
- authentic statements/witness testimony (WT)
- expert witness testimony (EWT)
- evidence of Recognition of Prior Learning (RPL).

Learners can use the abbreviations for cross-referencing purposes in their portfolios.

Learners can also use one piece of evidence to prove their knowledge, skills and understanding across different assessment criteria and/or across different units. It is not necessary for learners to have each assessment criterion assessed separately. They should be encouraged to reference evidence to the relevant assessment criteria. Evidence must be available to the assessor, internal verifier and Pearson standards verifier.

Any specific evidence requirements for individual units are stated in the unit introductions to the units.

There is further guidance about assessment on our website. Please see *Section 10* for details.

Credit transfer

Credit transfer describes the process of using a credit or credits awarded in the context of a different qualification or awarded by a different awarding organisation towards the achievement requirements of another qualification. All awarding organisations recognise the credits awarded by all other awarding organisations that operate within the QCF.

If learners achieve credits with other awarding organisations, they do not need to retake any assessment for the same units. The centre must keep evidence of credit achievement.

5 Centre resource requirements

As part of the approval process, centres must make sure that the resource requirements below are in place before offering the Pearson BTEC Level 4 Diploma in Information Security Professional Competence (QCF).

General resource requirements

- Centres must have the appropriate physical resources to support both the delivery and assessment of the qualification (for example, a workplace in line with industry standards, equipment, IT, learning materials and teaching rooms).
- Where permitted, a Realistic Working Environment (RWE) must offer the same conditions as the normal day-to-day working environment, with a similar range of demands, pressures and requirements for cost-effective working.
- Centres must meet any specific human and physical resource requirements. Staff assessing learners must meet the occupational competence requirements.
- There must be systems in place to ensure the continuing professional development for staff delivering the qualification.
- Centres must have appropriate health and safety policies, procedures and practices in place for the delivery of the qualification.
- Centres must deliver the qualifications in accordance with current equality legislation. For further details on Pearson's commitment to the Equality Act 2010, please see *Section 9 Access and recruitment* and *Section 10 Access to qualifications for learners with disabilities or specific needs*. For full details of the Equality Act 2010, please go to www.legislation.gov.uk

6 Centre recognition and approval centre recognition

Centres that have not previously offered this Pearson qualification need to apply for, and be granted, centre recognition as part of the process for approval to offer this individual qualification.

Guidance on seeking approval to deliver BTEC qualifications is given on our website, www.edexcel.com

Approvals agreement

All centres are required to enter into an approval agreement that is a formal commitment by the head or principal of a centre to meet all the requirements of the specification and any associated codes, conditions or regulations.

Pearson will act to protect the integrity of the awarding of qualifications. If centres do not comply with the agreement, this could result in the suspension of certification or withdrawal of approval.

7 Quality assurance of centres

Quality assurance is at the heart of vocational qualifications. Centres will internally assess Competence-based qualifications using internal quality assurance procedures to ensure standardisation of assessment across all learners. Pearson uses external quality assurance procedures to check that all centres are working to national standards. It gives us the opportunity to identify and provide support, if needed, to safeguard certification. It also allows us to recognise and support good practice.

For the qualifications in this specification, the Pearson quality assurance model is as described below.

Centres offering Pearson BTEC Competence-based qualifications will at least receive two standards verification visits per year. The exact frequency and duration of standards verifier visits must reflect the centre's performance, taking account of the number:

- of assessment sites
- and throughput of learners
- and turnover of assessors
- and turnover of internal verifiers.

For centres offering a full Pearson Apprenticeship (i.e. all elements of the Apprenticeship are delivered with Pearson through registration of learners on a Pearson Apprenticeship framework) a single standards verifier will be allocated to verify all elements of the Pearson Apprenticeship programme. If a centre is also offering stand-alone Competence-based qualifications in the same sector as a full Pearson Apprenticeship, the same standards verifier will be allocated.

In order for certification to be released, confirmation is required that the National Occupational Standards (NOS) for assessment, for internal verification and for the specific occupational sector are being consistently met.

Centres are required to declare their commitment to ensuring quality and to providing appropriate opportunities for learners that lead to valid and accurate assessment outcomes.

For further details, please go to the UK NVQ Quality Assurance Centre Handbook and the *Edexcel NVQs, SVQs and Competence-based qualifications – Delivery Requirements and Quality Assurance Guidance* on our website, at www.pearsonwbl.edexcel.com/NVQ-competence-based.

8 Programme delivery

Centres are free to offer the qualifications using any mode of delivery (for example full-time, part-time, evening only, distance learning) that meets learners' needs. Centres must have due regard to Pearson's policies that may apply to different modes of delivery.

Those planning the programme should aim to address the occupational nature of the qualification by:

- engaging with learners, initially, through planned induction, and subsequently through the involvement of learners in planning for assessment opportunities
- using naturally occurring workplace activities and products to present evidence for assessment against the requirements of the qualification
- developing a holistic approach to assessment by matching evidence to different assessment criteria, learning outcomes and units, as appropriate, thereby reducing the assessment burden on learners and assessors
- taking advantage of suitable digital methods to capture evidence.

9 Access and recruitment

Pearson's policy regarding access to its qualifications is that:

- they should be available to everyone who is capable of reaching the required standards
- they should be free from any barriers that restrict access and progression
- there should be equal opportunities for all wishing to access the qualifications.

Centres must ensure that their learner recruitment process is conducted with integrity. This includes ensuring that applicants have appropriate information and advice about the qualification to ensure that it will meet their needs.

Centres should review applicants' prior qualifications and/or experience, considering whether this profile shows that they have the potential to achieve the qualification.

For learners with disabilities and specific needs, this review will need to take account of the support available to the learner during teaching and assessment of the qualification. The review must take account of the information and guidance in *Section 10 Access to qualifications for learners with disabilities or specific needs*.

10 Access to qualifications for learners with disabilities or specific needs

Equality and fairness are central to our work. Pearson's Equality Policy requires all learners to have equal opportunity to access our qualifications and assessments. It also requires our qualifications to be awarded in a way that is fair to every learner.

We are committed to making sure that:

- learners with a protected characteristic (as defined by the Equality Act 2010) are not, when they are undertaking one of our qualifications, disadvantaged in comparison to learners who do not share that characteristic
- all learners achieve the recognition they deserve from undertaking a qualification and that this achievement can be compared fairly to the achievement of their peers.

Learners taking a qualification may be assessed in British Sign Language or Irish Sign Language where it is permitted for the purpose of reasonable adjustments.

Further information on access arrangements can be found in the Joint Council for Qualifications (JCQ) document *Access Arrangements, Reasonable Adjustments and Special Consideration for General and Vocational qualifications*.

Details on how to make adjustments for learners with protected characteristics are given in the document *Pearson Supplementary Guidance for Reasonable Adjustment and Special Consideration in Vocational Internally Assessed Units*.

Both documents are on our website at: www.edexcel.com/policies

11 Unit format

Units have the following sections.

Unit title

The unit title is on the QCF and this form of words will appear on the learner's Notification of Performance (NOP).

Unit reference number

Each unit is assigned a unit reference number that appears with the unit title on the Register of Regulated Qualifications.

QCF level

All units and qualifications within the QCF have a level assigned to them. There are nine levels of achievement, from Entry to Level 8. The QCF Level Descriptors inform the allocation of the level.

Credit value

When a learner achieves a unit, they gain the specified number of credits.

Guided learning hours

Guided learning hours are the times when a tutor, trainer or facilitator is present to give specific guidance towards the learning aim for a programme. This definition covers lectures, tutorials and supervised study in, for example, open learning centres and learning workshops. It also includes assessment by staff where learners are present. It does not include time spent by staff marking assignments or homework where the learner is not present.

Unit aim

This gives a summary of what the unit aims to do.

Essential resources

This section lists any specialist resources needed to deliver the unit. The centre will be asked to make sure that these resources are in place when it seeks approval from Pearson to offer the qualification.

Unit assessment requirements/evidence requirements

Learners must provide evidence according to each of the requirements stated in this section.

Learning outcomes

The learning outcomes of a unit set out what a learner knows, understands or is able to do as the result of a process of learning.

Assessment criteria

Assessment criteria specify the standard required by the learner to achieve each learning outcome.

Unit 101: Health and Safety in ICT

Unit reference number: Y/500/7183
QCF level: 1
Credit value: 3
Guided learning hours: 15

Unit aim

This unit explores compliance with health and safety legislation when working in ICT.

The basis of health and safety law is the Health and Safety at Work Act 1974. The act sets out the general duties that employers have towards employees and members of the public, and employees have to themselves and to each other.

What the law requires here is what good management and common sense would lead individuals and organisations to do anyway: that is, identify risks and take sensible measures to tackle them.

Health and safety legislation impacts not only on those who are employed at work, but on visitors, bystanders and customers who may be affected by actions of those engaged in work activities.

Health and safety legislation is subject to constant review, and new legislation is introduced on a regular basis. This constant change must be monitored by organisations and individuals to identify actions required to remain compliant. Interpretation of the legislation may also be modified as a result of case law or other legal guidance.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to comply with relevant health and safety procedures	1.1	Identify relevant organisational health and safety procedures			
		1.2	Identify available sources of health and safety information			
		1.3	Demonstrate how relevant health and safety procedures have been followed			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 303: Testing the Security of Information Systems

Unit reference number: T/505/5788
QCF level: 3
Credit value: 12
Guided learning hours: 40

Unit aim

On completion of this unit, learners will be able to conduct security tests and be able to report the results of tests using standard documents.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to conduct security testing	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			
2	Be able to report on test results	2.1	Examine the results of testing to identify security vulnerabilities			
		2.2	Prioritise identified vulnerabilities against specified information assurance requirement			
		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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature:_____ Date: _____
(*if sampled*)

Unit 304: Carrying Out Information Security Risk Assessment

Unit reference number: T/505/5791
QCF level: 3
Credit value: 9
Guided learning hours: 30

Unit aim

On completion of this unit, learners will be able to gather information, assess and report on the risks to information security.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to gather information on information security risks	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			
2	Be able to assess and report on information security risks	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 305: Investigating Information Security Incidents

Unit reference number: F/505/5793

QCF level: 3

Credit value: 9

Guided learning hours: 23

Unit aim

On completion of this unit, learners will be able to gather information to investigate, identify and report information security incidents.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to gather information to investigate information security incidents	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			
2	Be able to investigate information security incidents	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 306: Carrying Out Information Security Incident Management Activities

Unit reference number: F/505/5812

QCF level: 3

Credit value: 9

Guided learning hours: 25

Unit aim

On completion of this unit, learners will be able to carry out information security incident management activities and be able to gather information to manage incidents in information security.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to gather information to manage information security incidents	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			
2	Be able to carry out information security incident management activities	2.1	Identify types of actions required to resolve incidents or mitigate their impact			
		2.2	Report any incidents that 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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 307: Carrying Out Information Security Forensic Examinations

Unit reference number: R/505/5801
QCF level: 3
Credit value: 6
Guided learning hours: 10

Unit aim

This unit provides the relevant skills and methods for applying forensic examinations. On completion of this unit, learners will be able to report and undertake specific actions to secure relevant information in information security.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to carry out information security forensic examinations	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 308: Carrying Out Information Security Audits

Unit reference number: A/505/5808
QCF level: 3
Credit value: 6
Guided learning hours: 10

Unit aim

On completion of this unit, learners will be able to report, examine and follow organisational procedures on audit activities in information security.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to carry out information security audit activities	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 309: System Operation

Unit reference number: A/500/7340
QCF level: 3
Credit value: 12
Guided learning hours: 100

Unit aim

System operation is the ability to operate and monitor a system, which can be any combination of equipment, hardware and software. This may include:

- using data backup and restore routines
- handling of incidents
- controlling and monitoring availability and performance of system components
- start-up/close-down routines
- scheduling routine or preventative maintenance
- maintenance of operating plans and schedules.

Examples of 'operational activities' are:

- replenishment of consumables
- routine or preventative maintenance
- data backups.

A competent person at Level 3 can maintain and implement system operating procedures.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Know how to operate the system	1.1	Explain the operating procedures that are applicable to the system, such as: • required service levels (e.g. availability, quality) • routine maintenance • monitoring • data integrity (e.g. backups, antivirus) • consumables use, storage and disposal • health and safety • escalation • information recording and reporting • obtaining work permissions • security and confidentiality			
		1.2	Describe system functionality during normal operation			
		1.3	Describe the effects of operational activities on system functionality			

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Be able to operate systems	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: • loss or corruption of data • loss of service • damage to equipment • effects on customer operations			
3	Be able to maintain and implement system operating procedures	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 310: System Management

Unit reference number: D/500/7332
QCF level: 3
Credit value: 12
Guided learning hours: 100

Unit aim

System management is the ability to manage ICT systems to ensure that they deliver the required functionality and capacity. A system can be any combination of equipment, hardware and software.

System management could involve changing system configuration to meet short-term fluctuations in demand (for example, high numbers of calls to specific telephone numbers).

It could also involve longer-term changes such as increasing resources (for example, processing or storage capacity) to meet anticipated needs and taking account of advances in technology.

A competent person at Level 3 can administer a system.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Understand how to administer a system	1.1	Describe how to configure the system			
		1.2	Describe ICT asset and configuration information applicable to the system such as: • physical attributes (e.g. manufacturer, type, revision, serial number, location, value) • configuration (e.g. physical and logical addresses, options set, connections)			
		1.3	Describe how available options for system configuration affect functionality and capacity			
2	Be able to administer a system and change system configurations	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 311: Creating an Event-Driven Computer Program

Unit reference number: F/601/3179
QCF level: 3
Credit value: 12
Guided learning hours: 90

Unit aim

This unit covers the more advanced concepts of event-driven computer languages and their use to implement, refine and test computer programs.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to implement a software design using event-driven programming	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Be able to refine an event-driven program to improve quality	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			
3	Be able to test the operation of an event-driven program	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			
4	Be able to document an event-driven program	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 312: Creating an Object-Oriented Computer Program

Unit reference number: L/601/3184
QCF level: 3
Credit value: 12
Guided learning hours: 90

Unit aim

This unit covers the more advanced concepts of object-oriented computer languages and their use to implement, refine and test computer programs.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to implement a software design using object-oriented programming	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Be able to refine an object-oriented program to improve quality	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			
3	Be able to test the operation of an object-oriented driven program	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			
4	Be able to document an object-oriented driven program	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 313: Creating a Procedural Computer Program

Unit reference number: R/601/3171
QCF level: 3
Credit value: 12
Guided learning hours: 90

Unit aim

This unit covers the more advanced concepts of procedural computer languages and their use to implement, refine and test computer programs.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to implement a software design using procedural programming	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			
2	Be able to refine a procedural program to improve quality	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
3	Be able to test the operation of a procedural program	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			
4	Be able to document a computer program	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 314: Investigating and Defining Customer Requirements for ICT Systems

Unit reference number: R/601/3249
QCF level: 3
Credit value: 12
Guided learning hours: 75

Unit aim

This unit covers the investigation of existing systems and processes and the analysis of information to identify needs and constraints.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to investigate existing systems and processes	1.1	Use three of the following investigative methods: • observations • examination of existing documents, records or software • questionnaires • site surveys			
		1.2	Record the results of investigations using standard documentation			
		1.3	Explain the importance of preserving the confidentiality of customer information			
2	Be able to analyse information to identify needs and constraints	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 that can affect the design of an ICT system			
		2.3	Analyse information to identify customer needs for: • data to be stored and processed • functionality in terms of inputs, processes and outputs • 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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 315: User Profile Administration

Unit reference number: K/500/7379
QCF level: 3
Credit value: 9
Guided learning hours: 80

Unit aim

On completion of this unit learners will be able to administer user profiles.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Know how to administer user profiles	1.1	Describe the organisational policy on user profiles such as: user identifier (e.g. username) • password and related information (e.g. change frequency) • allowed system access (e.g. times, locations) • 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: • shared resources (e.g. data storage, printers) • software • data.			
2	Be able to administer user profile	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 401: Develop Own Effectiveness and Professionalism

Unit reference number: K/601/3502
QCF level: 4
Credit value: 12
Guided learning hours: 60

Unit aim

In this unit, learners will develop their own personal and professional IT security skills. They will understand professional practice and the legislative environment in an IT security context. Finally, learners will evaluate potential improvements to organisational effectiveness in a security context.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to develop own personal and professional skills	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			
2	Be able to work as a member of a team to achieve defined goals and implement agreed plans	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
3	Understand what is meant by professional practice	3.1	Interpret the implications, and applicability for IT professionals of: • Data Protection Act • 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			
4	Understand the ethical and legislative environment relating to IT activities	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: • processing of financial transactions • health and safety • privacy, confidentiality and security • copyright and intellectual property rights			
5	Be able to improve organisational effectiveness	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 403: Testing the Security of Information Systems

Unit reference number: A/505/5789
QCF level: 4
Credit value: 15
Guided learning hours: 60

Unit aim

On completion of this unit, learners will be able to plan and carry out security testing in relation to information security.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to plan security testing	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Be able to carry out security testing	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 404: Carrying Out Information Security Risk Assessment

Unit reference number: A/505/5792
QCF level: 4
Credit value: 12
Guided learning hours: 40

Unit aim

On completion of this unit, learners will be able to prepare and carry out information security risk assessment.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to prepare for information security risk assessments	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Be able to carry out information security risk assessments	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 405: Investigating Information Security Incidents

Unit reference number: D/505/5798
QCF level: 4
Credit value: 12
Guided learning hours: 35

Unit aim

On completion of this unit, learners will be able to prepare for information security incident investigations and manage information security incidents.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to prepare for information security incident investigations	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			
2	Be able to manage information security incidents	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 that 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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 407: Carrying Out Information Security Forensic Examinations

Unit reference number: M/505/5806
QCF level: 4
Credit value: 9
Guided learning hours: 20

Unit aim

On completion of this unit, learners will be able to carry out forensic examinations in information security.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to carry out information security forensic examinations	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 408: Carrying Out Information Security Audits

Unit reference number: A/505/5811
QCF level: 4
Credit value: 12
Guided learning hours: 30

Unit aim

On completion of this unit, learners will be able to prepare for and carry out audit activities for information security.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to prepare for information security audit activities	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			
2	Be able to carry out information security audit activities	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			

Learner name:_____ Date:_____

Learner signature:_____ Date:_____

Assessor signature:_____ Date:_____

Internal verifier signature: _____ Date:_____
(*if sampled*)

Unit 409: IT and Telecoms System Operation

Unit reference number: R/504/5513
QCF level: 4
Credit value: 15
Guided learning hours: 90

Unit aim

This unit enables learners to operate IT and telecoms systems. Learners will initially develop understanding of the technical architecture of either IT or telecoms systems and how to specify system operation parameters, and will then have the opportunity to control the operation and maintenance of systems.

Unit assessment requirements/evidence requirements

This unit must be assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Understand the technical architecture of IT or telecom systems	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Understand how to specify system operation parameters	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			
3	Be able to control the operation of systems	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
4	Be able to control system maintenance	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 410: IT and Telecoms System Management

Unit reference number: M/504/5504
QCF level: 4
Credit value: 15
Guided learning hours: 90

Unit aim

This unit enables learners to manage IT and telecoms systems, including configuring systems to meet organisational objectives and customer needs, risk evaluation and contributing to the development of an organisation's system management strategy.

Unit assessment requirements/evidence requirements

This unit must be assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Understand how to manage systems	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			
2	Be able to review the functionality and management of systems	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
3	Be able to manage systems	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 411: Designing and Developing Event-Driven Computer Program

Unit reference number: J/601/3300
QCF level: 4
Credit value: 15
Guided learning hours: 90

Unit aim

The aim of this unit is to provide the learner with the skills and competencies to carry out the development of an event-driven computer program from design to testing in a professional capacity, and to understand a range of issues concerned with software development activities.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to design event-driven programs to address loosely defined problems	1.1	Identify and structure the components and data required to address problems			
		1.2	Select and use predefined components, specialising as required			
		1.3	Identify the set of events that invoke behaviour of components and other program 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			
2	Be able to produce a working event-driven program which meets the design specification	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
3	Be able to develop event-driven programs that reflect established programming and software engineering practice	3.1	Apply standard naming, layout and comment conventions			
		3.2	Apply appropriate data validation and error handling techniques			
4	Be able to develop test strategies and apply these to event-driven programs	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			
5	Be able to develop design documentation for use in program maintenance and end-user documentation	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 412: Designing and Developing Object-Oriented Computer Program

Unit reference number: T/601/3308
QCF level: 4
Credit value: 15
Guided learning hours: 90

Unit aim

The aim of this unit is to provide the learner with the skills and competencies to carry out the development of an object-oriented computer program from design to testing in a professional capacity and to understand a range of issues concerned with software development activities.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to design object-oriented programs to address loosely defined problems	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			
2	Be able to produce a working object-oriented program which meets the design specification	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
3	Be able to develop object-oriented programs that reflect established programming and software engineering practice	3.1	Apply standard naming, layout and comment conventions			
		3.2	Apply appropriate data validation and error handling techniques			
4	Be able to develop test strategies and apply these to object-oriented programs	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			
5	Be able to develop design documentation for use in program maintenance and end-user documentation	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 413: Designing and Developing Procedural Computer Program

Unit reference number: T/601/3311
QCF level: 4
Credit value: 15
Guided learning hours: 90

Unit aim

The aim of this unit is to provide the learner with the skills and competencies to carry out the development of a procedural computer program from design to testing in a professional capacity, and to understand a range of issues concerned with software development activities.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to design procedural programs to address loosely defined problems	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			
2	Be able to produce a working procedural program which meets the design specification	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
3	Be able to develop procedural programs that reflect established programming and software engineering practice	3.1	Apply standard naming, layout and comment conventions			
		3.2	Apply appropriate data validation and error handling techniques			
4	Be able to develop test strategies and apply these to procedural programs	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			
5	Be able to develop design documentation for use in program maintenance and end-user documentation	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 414: Investigating and Defining Customer Requirements for ICT Systems

Unit reference number: R/602/1772

QCF level: 4

Credit value: 15

Guided learning hours: 90

Unit aim

This unit provides the skills, knowledge and understanding requirements to take a leading role in the investigation and definition of customer requirements for ICT systems and services.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to control the investigation of existing and proposed systems and processes	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Be able to analyse information to identify needs and constraints	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: • data to be stored and processed • functionality in terms of inputs, processes and outputs • 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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

Unit 415: Carrying out Information Security Risk Management

Unit reference number: L/505/5814
QCF level: 4
Credit value: 12
Guided learning hours: 40

Unit aim

On completion of this unit, learners will be able to manage and develop risk contingency plans and use these to manage information security risks.

Unit assessment requirements/evidence requirements

This unit is assessed in the workplace. Learners can enter the types of evidence they are presenting for assessment and the submission date against each assessment criterion. Alternatively, centre documentation should be used to record this information.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
1	Be able to develop information security risk contingency plans	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 outcomes		Assessment criteria		Evidence type	Portfolio reference	Date
2	Be able to manage information security risks	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			

Learner name: _____ Date: _____

Learner signature: _____ Date: _____

Assessor signature: _____ Date: _____

Internal verifier signature: _____ Date: _____
(*if sampled*)

12 Further information and useful publications

To get in touch with us visit our 'Contact us' pages:

- Edexcel: www.edexcel.com/contactus
- BTEC: www.edexcel.com/btec/Pages/Contactus
- Pearson Work Based Learning and Colleges: www.edexcel.com/about.wbl/Pages/Contact-us
- books, software and online resources for UK schools and colleges: www.pearsonschoolsandfecolleges.co.uk

Key publications:

- Adjustments for candidates with disabilities and learning difficulties – Access and Arrangements and Reasonable Adjustments, General and Vocational qualifications (Joint Council for Qualifications (JCQ))
- Equality Policy (Pearson)
- Recognition of Prior Learning Policy and Process (Pearson)
- UK Information Manual (Pearson)
- UK Quality Vocational Assurance Handbook (Pearson).

All of these publications are available on our website.

Publications on the quality assurance of BTEC qualifications are available on our website at www.edexcel.com/btec/delivering-BTEC/quality/Pages

Our publications catalogue lists all the material available to support our qualifications. To access the catalogue and order publications, please go to www.edexcel.com/resources/publications/Pages

Additional resources

If you need further learning and teaching materials to support planning and delivery for your learners, there is a wide range of BTEC resources available.

Any publisher can seek endorsement for their resources, and, if they are successful, we will list their BTEC resources on our website at: www.edexcel.com/resources/publications/Pages

13 Professional development and training

Pearson supports UK and international customers with training related to BTEC qualifications. This support is available through a choice of training options offered on our website: www.edexcel.com/resources/Training.

The support we offer focuses on a range of issues, such as:

- planning for the delivery of a new programme
- planning for assessment and grading
- developing effective assignments
- building your team and teamwork skills
- developing learner-centred learning and teaching approaches
- building in effective and efficient quality assurance systems.

The national programme of training we offer is on our website at: www.edexcel.com/resources/Training. You can request centre-based training through the website or you can contact one of our advisers in the Training from Pearson UK team via Customer Services to discuss your training needs.

BTEC training and support for the lifetime of the qualifications

Training and networks: our training programme ranges from free introductory events through sector-specific opportunities to detailed training on all aspects of delivery, assignments and assessment. We also host some regional network events to allow you to share your experiences, ideas and best practice with other BTEC colleagues in your region.

Regional support: our team of Curriculum Development Managers and Curriculum Support Consultants, based around the country, are responsible for providing advice and support in centres. They can help you with planning and curriculum developments.

To get in touch with our dedicated support teams please visit: www.edexcel.com/contactus

Online forum

Pearson Work Based Learning Communities is an online forum where employers, further education colleges and workplace training providers are able to seek advice and clarification about any aspect of our qualifications and services, as well as share knowledge and information with others. The forums are sector specific and cover Business Administration, Customer Service, Health and Social Care, Hospitality and Catering and Retail. The online forum is available at www.pearsonwbl.edexcel.com/Our-support.

14 Contact us

We have a dedicated Account Support team, based throughout the UK, to give you more personalised support and advice. To contact your Account Specialist you can use any of the following methods:

Email: wblcustomerservices@pearson.com
Telephone: 0844 576 0045

If you are new to Pearson and would like to become an approved centre, please contact us at:

Email: wbl@pearson.com
Telephone: 0844 576 0045

Complaints and feedback

We are working hard to provide you with excellent service. However, if any element of our service falls below your expectations, we want to understand why, so that we can prevent it from happening again. We will do all that we can to put things right.

If you would like to register a complaint with us, please email wblcomplaints@pearson.com.

We will formally acknowledge your complaint within two working days of receipt and provide a full response within seven working days.

July 2014

For more information on Edexcel and BTEC qualifications please visit our websites: www.edexcel.com and www.btec.co.uk