Pearson
BTEC Level 4 Certificate in Network Security

Specification

BTEC Professional qualification

First teaching June 2019

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 qualifications.pearson.com/contactus

About Pearson

Pearson is the world's leading learning company, with 35,000 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 qualifications.pearson.com

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.

ISBN 978 1 446 96083 7

Contents

1 Introducing BTEC Professional qualifications 1

What are BTEC Professional qualifications? 1

Sizes of BTEC Professional qualifications 1

2 Qualification summary and key information 3

3 Qualification purpose 5

Qualification objectives 5

Apprenticeships 5

Progression opportunities 6

Industry support and recognition 6

4 Qualification structures 7

Pearson BTEC Level 4 Certificate in Network Security 7

5 Centre resource requirements 8

General resource requirements 8

6 Access and recruitment 9

Prior knowledge, skills and understanding 9

Access to qualifications for learners with disabilities or specific needs 9

7 Programme delivery 11

8 Assessment 12

Language of assessment 12

External assessment 13

Sample assessment materials 14

Resits 14

Administrative arrangements for external assessment 14

Access arrangements requests 14

Granting reasonable adjustments 15

Special consideration requests 15

Conducting external assessments 15

Dealing with malpractice in assessment 16
External assessment 16
Learner malpractice 16
Teacher/centre malpractice 17
Sanctions and appeals 17

9 Centre recognition and approval 19

Approvals agreement 19

10 Unit 20

Unit 1: Network Security 22

11 Suggested teaching resources 32

12 Further information and useful publications 33

13 Professional development and training 34

1 Introducing BTEC Professional qualifications

What are BTEC Professional qualifications?

BTEC Professional qualifications are work-related qualifications available from Level 4 to Level 8 in a range of sectors. They give learners the knowledge, understanding and skills they need to prepare for employment in a specific occupational area. The qualifications also provide career development opportunities for those already in work.

BTEC Professional qualifications put learning into the context of the world of work, giving learners the opportunity to apply their research, skills and knowledge in relevant and realistic work contexts. This applied, practical approach means that learners develop the knowledge, understanding and skills they need for career progression or further study. As such, these qualifications are well-suited to support the delivery of the Apprenticeship Standards.

The qualifications may be offered as full-time or part-time courses in colleges and training centres, and through employers.

Sizes of BTEC Professional qualifications

For all regulated qualifications, Pearson specifies a total estimated number of hours that learners will require to complete and show achievement for the qualification – this is the Total Qualification Time (TQT). The TQT value indicates the size of a qualification.

Within the TQT, Pearson identifies the number of Guided Learning Hours (GLH) that we estimate a centre delivering the qualification might provide. Guided learning means activities, such as lessons, tutorials, online instruction, supervised study and giving feedback on performance, that directly involve tutors and assessors in teaching, supervising and invigilating learners. Guided learning includes the time required for learners to complete external assessment under examination or supervised conditions.

In addition to guided learning, other required learning directed by tutors or assessors includes private study, preparation for assessment and undertaking assessment when not under supervision, such as preparatory reading, revision and independent research.

As well as TQT and GLH, qualifications can also have a credit value – equal to one tenth of the TQT, rounded to the nearest whole number.

TQT and credit values are assigned after consultation with employers and training providers delivering the qualifications.

BTEC Professional qualifications are generally available in the following sizes:

- Award – a qualification with a TQT value of 120 or less (equivalent to a range of 1–12 credits)
- Certificate – a qualification with a TQT value in the range of 121–369 (equivalent to a range of 13–36 credits)
- Diploma – a qualification with a TQT value of 370 or more (equivalent to 37 credits and above).

2 Qualification summary and key information

Qualification title	Pearson BTEC Level 4 Certificate in Network Security
Qualification Number (QN)	603/4685/1
Regulation start date	29/05/2019
Operational start date	01/06/2019
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. Please see *Section 6 Access and recruitment*.
Total Qualification Time (TQT)	150 hours.
Guided Learning Hours (GLH)	50.
Assessment	External assessment – multiple-choice test
Grading information	The qualification and unit is at a Pass grade.
Entry requirements	No prior knowledge, understanding, skills or qualifications are required before learners register for this qualification. However, it is recommended that learners have experience of working in the digital sector or that they have achieved a relevant qualification, for example a Level 3 information and communication technologies qualification. Centres must follow the guidance given in our document *A guide to recruiting learners onto Pearson qualifications* (see *Section 6 Access and recruitment*).
Funding	Qualifications eligible and funded for post-16-year-olds can be found on the funding Hub. The Skills Funding Agency also publishes a funding catalogue that lists the qualifications available for 19+ funding. The Apprenticeship funding rules can be found at www.gov.uk

Centres will need to use the Qualification Number (QN) when they seek public funding for their learners. The qualification title, unit titles and QN will appear on each learner's final certificate. Centres should tell learners this when recruiting them and registering them with Pearson. There is more information about certification in our *UK Information Manual,* available on our website, qualifications.pearson.com

3 Qualification purpose

Qualification objectives

The Pearson BTEC Level 4 Certificate in Network Security develops the knowledge and understanding learners need to carry out the job role of Network Engineer, relating to network security. The qualification also enables learners to achieve one of the knowledge modules required to complete the on-programme element on the Network Engineer Apprenticeship.

The qualification gives learners the opportunity to:

- develop knowledge related to network engineering
- develop technical knowledge and understanding in network security
- achieve a level 4 qualification
- develop personal growth and engagement in learning.

Apprenticeships

The Pearson BTEC Level 4 Certificate in Network Principles meets one of the mandatory gateway requirements within the Network Engineer Apprenticeship Standard.

Learners must achieve this qualification, one of the equivalent professional Ofqual regulated qualifications, or one of the equivalent vendor qualifications before progressing to the end-point assessment. The equivalent vendor qualifications are:

- CCNA Security
- Juniper
- MTA Cloud and Mobility
- Security +.

The Pearson BTEC Level 4 Certificate in Network Security covers the following knowledge outcome from the Network Engineer Apprenticeship Standard:

- understands and responds to security threats, firewalls and vulnerabilities.

Progression opportunities

Learners who achieve the qualification and who have met all other specified requirements of the Network Engineer Apprenticeship Standard, including end-point assessment, can progress to achieving the full apprenticeship certification, which confirms competency in the Network Engineer job role.

With further training and development, learners can progress to a more senior or complex job role such as IT Network Manager. Learners will also be eligible to apply for registration to the Register of IT Technicians, confirming Skills Framework for the Information Age (SFIA) Level 3 professional competence on completing the apprenticeship.

Alternatively, learners who have achieved the qualification, but who have not completed the full apprenticeship requirements, could progress to a job role such as IT Infrastructure Technician or to another qualification such as the Pearson BTEC Level 5 Higher National Diploma in Computing.

Industry support and recognition

This qualification is based on the requirements set out in the Network Engineer Apprenticeship Standard issued by the Tech Partnership.

The employers involved in creating the Standard are:

Arqiva, BT, Capgemini, Cisco, Freedom Communications, Her Majesty's Revenue and Customs (HMRC), HP Inc. (formerly Hewlett-Packard), the Home Office, IBM, John Lewis plc, Microsoft, the National Health Service (NHS), Optimity, Oracle, the RAF, The Royal Corps of Signals

The qualification is supported by The Computing Technology Industry Association (CompTIA).

4 Qualification structure

Pearson BTEC Level 4 Certificate in Network Security

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

Minimum number of units that must be achieved	1

Unit number	Mandatory unit	Level	Guided Learning Hours
1	Network Security	4	50

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 qualifications.

General resource requirements

- Centres must have appropriate physical resources (for example IT, learning materials, teaching rooms) to support the delivery and assessment of the qualification.
- Staff involved in the assessment process must have relevant expertise and occupational experience.
- There must be systems in place that ensure continuing professional development (CPD) for staff delivering the qualification.
- Centres must have appropriate health and safety policies in place that relate to the use of equipment by learners.
- 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 6 Access and recruitment*. For full details of the Equality Act 2010 visit www.legislation.gov.uk

For information on the requirements for implementing assessment processes in centres, please refer to the *BTEC UK Quality Assurance Centre Handbook* available on our website.

6 Access and recruitment

Our policy on access to our qualifications is that:

- they should be available to everyone who is capable of reaching the required standards
- they should be free from 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.

We refer centres to the Pearson *Equality, diversity and inclusion policy*, which can be found in the support section of our website.

Prior knowledge, skills and understanding

No prior knowledge, understanding, skills or qualifications are required before learners can register for this qualification. However, it is recommended that learners have experience of working in the digital sector or that they have achieved a relevant qualification, such as a level 3 information and communication technologies qualification.

Access to qualifications for learners with disabilities or specific needs

Equality and fairness are central to our work. Pearson's *Equality, diversity and inclusion policy* document requires all learners to have equal opportunity to access our qualifications and assessments and that our qualifications are 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.

For learners with disabilities and specific needs, the centres' assessment of their potential to achieve the qualification must identify, where appropriate, the support that will be made available to them during delivery and assessment of the qualification. Please see *Section 8 Assessment* for information on reasonable adjustments and special consideration.

7 Programme delivery

Centres are free to offer this qualification using any mode of delivery that meets learners' and employers' needs. It is recommended that centres make use of a wide range of training delivery methods, including direct instruction in classrooms, simulated demonstrations, research or applied projects, e-learning, directed self-study, field visits and role play. Whichever mode of delivery is used, centres must make sure that learners have access to the resources identified in the specification and to the subject specialists delivering the units.

Centres must adhere to the Pearson policies that apply to the different models of delivery. Our document, *Collaborative and consortium arrangements for the delivery of vocational qualifications policy* is available on our website.

Those planning the programme should aim to enhance the vocational nature of the qualification by:

- spending time with employers to better understand their organisational requirements and the methods of training that are most suitable, taking into consideration their available resources and working patterns
- collaborating with employers to ensure that learners have opportunities in the workplace to implement the knowledge and skills developed through the training programme
- developing up-to-date and relevant teaching materials that make use of scenarios relevant to the sector and relevant occupation
- giving learners the opportunity to apply their learning in realistic practical activities
- having regular meetings with employers to discuss learner progress, providing feedback and agreeing how any issues will be resolved
- making full use of the variety of experience of work and life that learners bring to the programme.

Where legislation is taught, centres must ensure that it is current and up to date.

Where a unit is externally assessed, it is essential that learners have covered all of the unit content before they are tested.

For further information on the delivery and assessment of the Apprenticeships Standards please refer to document, *Apprenticeship funding: rules and guidance for employers* at:
www.gov.uk/government/collections/sfa-funding-rules

8 Assessment

The table below gives a summary of the assessment methods used in the qualification.

Units	Assessment method
Unit 1	External assessment (onscreen test).

In administering external assessments, centres need to be aware of the specific procedures and policies that apply to, for example, registration, entries and results. More information can be found in our *UK Information Manual*, available on our website.

Language of assessment

External assessments for the unit in this qualification will be available in English only.

Further information on the use of language in qualifications is available in our *Use of languages in qualifications policy* document, available on our website.

For further information on access arrangements, please refer to the *Granting reasonable adjustments* paragraph.

External assessment

The table below gives information about the type and availability of external assessments that are available for this qualification. Centres should check this information carefully together with the relevant unit specifications and the sample assessment materials so that they can timetable learning and assessment periods appropriately.

Unit 1: Network Security	
Type of assessment	Onscreen test using multiple-choice items.
Length of assessment	The external assessment will be 1 hour.
Number of marks	30
Assessment availability	On demand
First assessment availability	October 2019

Pearson sets and marks the external assessment.

The external assessment assesses all the learning outcomes in the unit to meet the standard specified by the related assessment criteria. All the content in the unit is mandatory for the assessment and will be sampled across different versions of the assessment over time. Therefore, it is essential that learners have full knowledge of the unit content before being entered for the onscreen test.

Centres need to make sure that learners are:

- fully prepared to sit the external assessment
- entered for the test at appropriate time, with due regard for resit opportunities as necessary.

Information on the structure and format of the assessment is available in *Section 10 Unit*.

Information on registering learners for the test and the systems requirements for delivering the onscreen test is available on our website.

Sample assessment materials

The unit is externally assessed and has a set of sample assessment materials (SAMs). The SAMs are there to provide an example of what the external assessment will look like in terms of the feel and level of demand of the assessment.

SAMs show the range of possible question types that may appear in the actual assessment and give a good indication of how the assessment will be structured.

While SAMs can be used for practice with learners as with any assessment the content covered and specific details of the questions asked will change in each assessment.

A copy of the assessment can be downloaded from the qualification page on our website.

Resits

Learners who take the onscreen test and do not perform as expected are allowed the opportunity to resit the assessment. Opportunities for resits are available purely at the centre or employer's discretion. Centres will need to ensure that learners are fully prepared for any identified areas of weakness before resitting the assessment.

Administrative arrangements for external assessment

Access arrangements requests

Access arrangements are agreed with Pearson before an assessment. They allow learners with special educational needs, disabilities or temporary injuries to:

- access the assessment
- show what they know and can do without changing the demands of the assessment.

Access arrangements should always be processed at the time of registration.

Learners will then know the type of arrangements available for them.

Granting reasonable adjustments

For external assessment, a reasonable adjustment is one that Pearson agrees to make for an individual learner. A reasonable adjustment is defined for the individual learner and is informed by the list of available access arrangements.

Whether an adjustment will be considered reasonable will depend on a number of factors, including:

- the needs of the learner with the disability
- the effectiveness of the adjustment
- the cost of the adjustment; and
- the likely impact of the adjustment on the learner with the disability and other learners.

Adjustment may be judged unreasonable and not approved if it involves unreasonable costs, timeframes or affects the integrity of the assessment.

Special consideration requests

Special consideration is an adjustment made to a learner's mark or grade after an external assessment to reflect temporary injury, illness or other indisposition at the time of the assessment.

An adjustment is made only if the impact on the learner is such that it is reasonably likely to have had a material effect on that learner being able to demonstrate attainment in the assessment.

Centres are required to notify us promptly of any learners who they believe have been adversely affected and request that we give special consideration. Further information can be found in the special requirements section on our website.

Conducting external assessments

Centres must make arrangement for the secure delivery of external assessments. All centres offering external assessments must comply with the Joint Council for Qualifications (JCQ) document *Instructions for conducting examinations*. The current version of this document is available on our website.

Dealing with malpractice in assessment

Malpractice means acts that undermine the integrity and validity of assessment, the certification of qualifications and/or may damage the authority of those responsible for delivering the assessment and certification.

Pearson does not tolerate actual or attempted malpractice by learners, centre staff or centres in connection with Pearson qualifications. Pearson may impose penalties and/or sanctions on learners, centre staff or centres where malpractice or attempted malpractice has been proven.

Malpractice may occur or be suspected in relation to any unit or type of assessment within a qualification. For further details on malpractice and advice on preventing malpractice by learners, please see the document *Centre guidance: Dealing with malpractice and maladministration in vocational qualifications*, available on our website.

The procedures we ask you to adopt vary between units that are internally assessed and those that are externally assessed.

External assessment

External assessment means all aspects of units that are designated as external in this specification, including preparation for tasks and performance. For these assessments, centres must follow the JCQ procedures set out in the latest version of the Joint Council for Qualifications (JCQ) document *Suspected malpractice in examinations and assessments – Policies and procedures* (available on the JCQ website, www.jcq.org.uk).

In the interests of learners and centre staff, centres need to respond effectively and openly to all requests relating to an investigation into an incident of suspected malpractice.

Learner malpractice

The head of centre is required to report incidents of suspected learner malpractice that occur during Pearson examinations. We ask centres to complete JCQ Form M1 (www.jcq.org.uk/malpractice) and email it with any accompanying documents (signed statements from the learner, invigilator, copies of evidence, etc) to the Investigations Processing team at candidatemalpractice@pearson.com.

The responsibility for determining appropriate sanctions or penalties to be imposed on learners lies with Pearson.

Learners must be informed at the earliest opportunity of the specific allegation and the centre's malpractice policy, including the right of appeal. Learners found guilty of malpractice may be disqualified from the qualification for which they have been entered with Pearson.

Teacher/centre malpractice

The head of centre is required to inform Pearson's Investigations team of any incident of suspected malpractice by centre staff, before any investigation is undertaken. The head of centre is requested to inform the Investigations team by submitting a JCQ M2(a) form (downloadable from www.jcq.org.uk/malpractice) with supporting documentation to pqsmalpractice@pearson.com. Where Pearson receives allegations of malpractice from other sources (for example Pearson staff, anonymous informants), the Investigations team will conduct the investigation directly or may ask the head of centre to assist.

Incidents of maladministration (errors in the delivery of Pearson qualifications that may affect the assessment of learners) should also be reported to the Investigations team using the same method.

Heads of centres/principals/chief executive officers or their nominees are required to inform learners and centre staff suspected of malpractice of their responsibilities and rights, please see 6.15 of the Joint Council for Qualifications (JCQ) document *Suspected malpractice in examinations and assessments – Policies and procedures.*

Pearson reserves the right in cases of suspected malpractice to withhold the issuing of results/certificates while an investigation is in progress. Depending on the outcome of the investigation, results and/or certificates may not be released or they may be withheld.

We reserve the right to withhold certification when undertaking investigations, audits and quality assurances processes. You will be notified within a reasonable period of time if this occurs.

Sanctions and appeals

Where malpractice is proven, we may impose sanctions or penalties.

Where learner malpractice is evidenced, penalties may be imposed such as:

- mark reduction for affected external assessments
- disqualification from the qualification
- debarment from registration for Pearson qualifications for a period of time.

If we are concerned about your centre's quality procedures we may impose sanctions such as:

- working with centres to create an improvement action plan
- requiring staff members to receive further training
- placing temporary blocks on the centre's certificates
- placing temporary blocks on the registration of learners
- debarring staff members or the centre from delivering Pearson qualifications
- suspending or withdrawing centre approval status.

The centre will be notified if any of these apply.

Pearson has established procedures for centres that are considering appeals against penalties and sanctions arising from malpractice. Appeals against a decision made by Pearson will normally be accepted only from the head of centre (on behalf of learners and/or members or staff) and from individual members (in respect of a decision taken against them personally). Further information on appeals can be found in our document *Enquiries and appeals about Pearson vocational qualifications and end point assessment policy,* available on our website. In the initial stage of any aspect of malpractice, please notify the Investigations Team (via pqsmalpractice@pearson.com) who will inform you of the next steps.

9 Centre recognition and approval

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

Existing centres will be given 'automatic approval' for a new qualification if they are already approved for a qualification that is being replaced by a new qualification and the conditions for automatic approval are met.

Centres offering mandatory qualifications for Apprenticeship Standards must be listed on the Skills Funding Agency's Register of Training Organisations and have a contract to deliver them.

Guidance on seeking approval to deliver BTEC qualifications is given on our website.

Approvals agreement

All centres are required to enter into an approval agreement with Pearson, in which the head of centre or principal agrees to meet all the requirements of the qualification specification and to comply with the policies, procedures, codes of practice and regulations of Pearson and relevant regulatory bodies. If centres do not comply with the agreement, this could result in the suspension of certification or withdrawal of centre or qualification approval.

10 Unit

This section explains how the unit is structured. It is important that all tutors, assessors, internal verifiers and other staff responsible for the programme review this section

Units have the following sections.

Unit number

The number is in a sequence in the specification.

Unit title

This is the formal title of the unit that will appear on the learner's certificate. Where a specification has more than one qualification, numbers may not be sequential for an individual qualification.

Level

All units and qualifications have a level assigned to them. The level assigned is informed by the level descriptors defined by Ofqual, the qualifications regulator.

Guided Learning Hours (GLH)

This indicates the number of hours of activities that directly or immediately involve tutors and assessors in teaching, supervising, and invigilating learners, for example lectures, tutorials, online instruction and supervised study.

Pearson has consulted with users of the qualification and has assigned a number of hours to this activity for the unit in this specification.

Unit introduction

This is designed with learners in mind. It indicates why the unit is important, what will be learned and how the learning might be applied in the workplace.

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

The assessment criteria specify the standard the learner is required to meet to achieve a learning outcome.

Unit content

This section sets out the required teaching content of the unit and specifies the knowledge and understanding required for achievement of the unit. It enables centres to design and deliver a programme of learning that will enable learners to achieve each learning outcome and to meet the standard determined by the assessment criteria.

Where it is designed to support apprenticeships, the unit content is informed by the knowledge and understanding requirements of the relevant Apprenticeship Standard.

Relationship between unit content and assessment criteria

All the content in each unit is mandatory for the assessments and will be sampled across different versions of the assessment over time. Learners can be tested on any aspect of the content.

Learners should be asked to complete summative assessment only after the teaching content for the unit or learning outcomes has been covered.

Legislation

Legislation cited in the units is current at time of publication. The most recent legislation should be taught and assessed internally. External assessments will use the most recent legislation.

Essential information for tutors and assessors

This section gives information to support delivery and the implementation of assessment. It contains the following subsection.

- *Essential resources* – 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 1: Network Security

Level: 4

Guided learning hours: 50

Unit introduction

The aim of this unit is to ensure that learners understand that networks are regularly subjected to a variety of threats that could lead to data being compromised or to an organisation being unable to carry out its primary function. Learners will develop an understanding of how these threats can be mitigated by using a range of tools and techniques.

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	
1	Understand the underpinning concepts of network security	1.1	Explain how concepts of network security are applied
		1.2	Describe network vulnerabilities
		1.3	Describe sources of threats to networks and systems
		1.4	Describe actions carried out when compromising networks
		1.5	Explain the impacts of an attack on networks and organisations
2	Understand responses to network security issues	2.1	Describe the stages undertaken as part of a risk management strategy
		2.2	Explain the use of risk management processes
		2.3	Describe the principles of current legislation and standards relating to cyber security
3	Understand how to mitigate threats	3.1	Describe the use of software tools when mitigating against threats
		3.2	Describe the use of hardware tools when mitigating against threats
		3.3	Describe the use of common encryption methods
		3.4	Describe the use of physical and corporate measures to control access

Unit content

What needs to be learned
Learning outcome 1: Understand the underpinning concepts of network security

Explain how concepts of network security are applied
• CIA (confidentiality, integrity and availability) triad (provides framework for the implementation of network security):
  ○ confidentiality (document classification, permissions)
  ○ integrity
  ○ availability.
• IAAA model (identification, authentication, authorisation and auditing).
• Access control (mandatory access control (MAC)), discretionary access control (DAC), attribute based access control (ABAC), role-based access control (RBAC)).
• Non-repudiation (hashing, digital signatures).
Describe network vulnerabilities
• Misconfigured devices (end point devices, interconnection devices).
• Weak passwords (complexity, aging).
• Unpatched software, unpatched firmware (errors in code, known security issues, legacy systems).
• Unencrypted data (interception, eavesdropping, loss of sensitive information).
• Errors in the code (intentional, backdoor/trapdoor, buffer overflow).
• Open Ports (access to software, access to data).

What needs to be learned

Describe sources of threats to networks and systems

- Actors:
  - hackers (black hat, grey hat, white hat, script kiddie, hacktivists)
  - employees (disgruntled, untrained, incompetent)
  - state sponsored actors
  - criminals
  - competitors.
- Viruses, ransomware, adware, spyware, keylogger, trojan, logic bomb, worm, rootkit (email, websites, removable storage, downloads).
- Brute force attack, dictionary attack, domain naming system (DNS) poisoning, dynamic host configuration protocol (DHCP) hijacking, IP/MAC address spoofing, man-in-the middle (MITM) attacks, bluejacking, bluesnarfing, SIM cloning, address resolution protocol (ARP) poisoning (hacker).
- Cookies (websites).
- Denial of service (DoS), distributed denial of service (DDoS) (botnets, zombies).
- Social engineering (baiting, phishing, spear phishing, pretexting).
- Structured query language (SQL) injection (database, websites, user login interface).
- Employee's personal devices (bring your own device (BYOD)).

Describe actions carried out when compromising networks

- Gaining unauthorised access to data.
- Corruption of data.
- Deletion of data.
- Alteration of data (during transmission and storage, man-in-the-middle (MITM)).
- Holding data to ransom.
- Denying services (flooding).
- Impersonation of legitimate IP / MAC addresses.
- Altering system settings (denial of access).
- Scanning ports.
- Introduction of unauthorised software to systems (adware, spyware, applications).
- Social engineering (phishing, spear phishing, pre-texting, shoulder surfing).

What needs to be learned

Explain the impacts of an attack on networks and organisations

- Loss of data required to undertake business processes.
- Diminished reputation (lack of client engagement, no longer recommended by current clients).
- Financial penalties for non-compliance with legislation (data protection, misuse of computers).
- Reduced profits (loss of financial details, paying to gain access to data being held by third party, fraud).
- Increased overheads (hardware, specialist support).
- Denial of services (access to websites, ability to place orders, access to data stored on networks).

What needs to be learned

Learning outcome 2: Understand responses to network security issues

Describe the stages undertaken as part of a risk management strategy

- Identify the risk (threat, vulnerability, assets concerned) .
- Analyse the risk (likelihood of occurrence, potential impact, risk rating, identification of potential solutions).
- Evaluate the risk (mean time to recovery (MTTR), mean time between failures (MTBF), recovery time objectives, recovery point objectives.
- Mitigate against the risk (reactive mitigation).
- Monitor & review the risk (security audits, security baselines).

Explain the use of risk management processes

- Tools used in risk management:
    - fault tree analysis
    - failure mode effect critical analysis (FMECA)
    - Central Computer and Telecommunications Agency (CCTA)
    - risk analysis and management methodologies.
- Threat assessment (environmental, manmade, internal, external):
    - define scope of threat
    - review existing policies
    - carry out testing (vulnerability, penetration)
    - determine likelihood of threat occurring
    - plan controls
    - implement controls
    - monitor controls.
- Threat modelling:
    - manual and automated processes
    - selection criteria (size of network, budgetary constraints, available resource).
- Risk assessment:
    - internal (asset value, potential threats, impact of threats)
    - external (supply chain assessments).

What needs to be learned

- Penetration testing (application, network, physical):
    - planning
    - discovery
    - attack
    - reporting.
- Vulnerability scanning (passive and active scanners, architecture exposure, compatibility).
- Risk response (accept, transfer, avoid, mitigate).

Describe the principles current legislation and standards relating to cyber security

- Information Systems Audit and Control Association (ISACA) risk IT framework (IT governance).
- Control Objectives for Information and Related Technologies (COBIT) framework (IT governance and compliance).
- Responsible, accountability, consulted, informed (RACI) (the four key responsibilities).
- ISO 27001 standard (compliance).
- National Cyber Security Centre (NCSC) 10 Steps to Cyber Security (education and compliance).
- Centre for Internet Security (CIS) benchmarks (compliance and guidance).
- Data protection legislation (lawful processing of data, roles and responsibilities of individuals and organisations, access to personal data, ensures validity of data, storing data).
- Computer misuse legislation (misuse of personal data, misuse of equipment, misuse of systems).
- Bring your own device (BYOD) policy (permissions required to access networks, websites that can be accessed, responsibilities of individuals and organisations).

What needs to be learned

Learning outcome 3: Understand how to mitigate threats

Describe the use of software tools when mitigating against threats

- Software firewalls (port blocking, stateful inspection, stateless inspection).
- Anti-Virus (virus definition, networked, stand-alone, scanning, scheduling).
- Blockchain (decentralised ledger, mathematical calculations to validate transactions).
- Spam filters (filtering emails based on definitions).
- Directory services (users, groups, permissions, access control lists (ACLs), multi-factor authentication).
- System hardening (closing unused ports, disabling unused services).
- Data backup (full, incremental, differential, snapshots, cloning, imaging).
- File permissions (new technology file system (NTFS), Sharing, Linux – Read, write, execute, -,+).
- Protocol analysers (gathering and analysing data packets).

Describe the use of hardware tools when mitigating against threats

- Hardware firewalls (port blocking, stateful inspection, stateless inspection).
- Demilitarised zone (DMZ) (isolating vulnerable components of the network).
- Network address translation (NAT) (converting public IP addresses to private IP addresses and vice versa).
- Port address translation (PAT) (port forwarding).
- Intrusion detection systems (IDS) (host-based intrusion detection system (HIDS), network-based intrusion detection system (NIDS)).
- Intrusion prevention systems (IPS) (rule based prevention).
- Switches (media access control (MAC) address filtering, virtual LANs (VLANs)).
- Routers (access control lists (ACLs), password protecting access).
- Data backup (hot, warm and cold backup sites, cloud).
- Redundancy (redundant array of inexpensive disks (RAID) 1, 5 & 10, failover, clustering).
- Honeypot (a single device).
- Honeynet (multiple devices).

What needs to be learned

Describe the use of common encryption methods

- Securing data transmissions using public networks (virtual private network (VPN), tunnelling, open VPN, L2TP, PSec, SSTP).
- Securing traffic between browsers and websites (secure socket layer (SSL), transport layer security (TLS), hypertext transfer protocol secure) (HTTPS)).
- Securing data on wireless networks (WI-FI Protected Access (WPA, WPA2, WPA3) number bits used for encryption, pre-shared keys, simultaneous authentication of equals, adaptive security appliance (ASA)).
- Securing data during transmission:
    - asymmetric encryption (Rivest, Shamir, Adleman (RSA), digital signature algorithm (DSA) Public key cryptography standards (PKCS))
    - symmetric encryption (advanced encryption standard (AES), bowfish, twofish, data encryption standard (DES), triple DES).
- Securing data on local storage (whole disk encryption, AES encryption, cipher block chaining (CBC), temporal keys, whole disc encryption).
- Ensuring integrity of data (hashing).

Describe the use of physical and corporate measures to control access.

- Physical:
    - biometrics (controlling access to resources and areas using retina, finger print, facial recognition, voice recognition)
    - locks (cypher pads, swipe cards/key fobs (RFID), mortice)
    - closed circuit television (CCTV) (monitoring access to controlled areas)
    - fences (preventing access to restricted areas)
    - reception/security personnel (controlling access to restricted areas).
- Corporate:
    - policies and procedures (password policies, end user polices, user acceptance policies, BOYD policies and procedures, human resource policies)
    - staff training and awareness (application-specific training, data protection, induction training, updates on policies on procedures).

Essential information for tutors and assessors

Essential resources

There are no special resources needed for this unit.

Assessment

This section must be read in conjunction with *Section 8 Assessment*.

This unit is externally assessed through an onscreen test that is set and marked by Pearson. The test lasts for 60 minutes and is worth 30 marks. The assessment is available on demand.

The test assesses all of the learning outcomes. The questions in the test are based on each assessment criterion and its associated unit content.

The test consists of the multiple-choice items.

Items in the test will not necessarily be sequenced in the order of the criteria in the unit. Test items will not rely on or directly follow on from another test item. Test items may use colour images/diagrams/graphs for the context of the question or for the answer options.

A Pass grade is determined by learners achieving a defined cut score (pass mark).

11 Suggested teaching resources

This section lists resource materials that can be used to support the delivery of the unit.

Textbooks

Dulaney E, Easttom C - *CompTIA Security+ Study Guide: Exam SY0-501* (Sybex 2017) ISBN 9781119416876

Evans L - *Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare* (independently published, 2018) ISBN 9781791553586

Evans L - *What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners* (independently published, 2019) ISBN 9781794647237

12 Further information and useful publications

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

- Edexcel, BTEC and Pearson Work Based Learning contact details: qualifications.pearson.com/en/support/contact-us.html
- Books, software and online resources for UK schools and colleges: www.pearsonschoolsandfecolleges.co.uk

Key publications

- *Access arrangements and reasonable adjustments* (Joint Council for Qualifications (JCQ))
- *A guide to recruiting learners onto Pearson qualifications* (Pearson)
- *A guide to the special consideration process* (JCQ)
- *BTEC UK Quality Assurance Centre Handbook* (Pearson)
- *Collaborative and consortium arrangements for the delivery of vocational qualifications policy* (Pearson)
- *Enquiries and appeals about Pearson vocational qualifications and end point assessment policy* (Pearson)
- *Equality, diversity and inclusion policy* (Pearson)
- *Suspected malpractice in examinations and assessments – Policies and procedures* (JCQ)
- *UK Information Manual* (Pearson)
- *Use of languages in qualifications policy* (Pearson).

All of these publications are available on our website.

Publications on the quality assurance of BTEC qualifications are also available on our website.

Our publications catalogue lists all the material available to support our qualifications. To access the catalogue and order publications, please visit our website.

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.

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.

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. 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 our website.

Your Pearson support team

Whether you want to talk to a sector specialist, browse online or submit your query for an individual response, there's someone in our Pearson support team to help you whenever – and however – you need:

- Subject Advisors: find out more about our subject advisor team – immediate, reliable support from a fellow subject expert
- Ask the Expert: submit your question online to our Ask the Expert online service and we will make sure your query is handled by a subject specialist.

Please visit our website at qualifications.pearson.com/en/support/contact-us.html

TSet060619 9781446960837_BTEC_PRO_L4_NETSEC.1-39/1

July 2019

For information about Pearson Qualifications, including Pearson Edexcel, BTEC and LCCI qualifications visit qualifications.pearson.com