Pearson BTEC

L3

Pearson BTEC
Level 3 Technical Occupational Entry for

Cyber Security Technician (Diploma)

Specification

First teaching from August 2025
First certification from 2026

Issue 1

Qualification Number: 610/3933/0

Pearson BTEC Level 3 Technical Occupational Entry for Cyber Security Technician (Diploma)

Specification

BTEC Technical Qualification

First registration August 2025

About Pearson

We are the world's leading learning company operating in countries all around the world. We provide content, assessment and digital services to students, educational institutions, employers, governments, and other partners globally. We are committed to helping equip students with the skills they need to enhance their employability prospects and to succeed in the changing world of work. We believe that wherever learning flourishes so do people.

Publication code: VQ000350

Welcome

With a track record built over 30 years of student success, BTEC qualifications are widely recognised and respected. They provide progression to the workplace either directly or via study at higher levels. Recent data has shown that 1 in 5 adults of working age in the UK has a BTEC qualification.

Why choose BTEC Level 3 Technical Qualifications?

BTEC Level 3 Technical Qualifications enable students to develop a purposeful and coherent combination of knowledge, skills and behaviours to confidently enter or progress into employment in occupations that are recognised and demanded by employers.

The qualifications, which are based on the occupational standards published by the Institute for Apprenticeships and Technical Education (IfATE), embody a fundamentally student-centred approach to the curriculum, with a flexible, unit-based structure and an approach to learning and assessment that:

- provides students with meaningful and occupationally relevant learning experiences
- engages and motivates students to achieve as assessments can be focused on individual student needs and can be achieved as they progress through the qualifications
- promotes self-directed learning through the clarity and transparency of the standards to be achieved
- makes the qualifications accessible to a wider range of students, including part time and adult students.

In developing these qualifications, we have collaborated with employers to ensure that the qualifications meet the current and emerging needs of industry. We have also worked with colleges and training providers to ensure that the qualifications meet their needs and those of their students.

We are providing a range of support to ensure that students and their tutors have the best possible experience during their course. Further information is provided on the qualification pages of our website.

A word to students

This qualification will require commitment and hard work. You will have to complete the learning for the required range of units, be organised, and complete your assessments, which may include practical work-based activities, projects, and vocational assignments. But you can feel proud to achieve a BTEC Level 3 Technical Qualification as you can be confident in your readiness to advance your career in your chosen occupation.

Good luck, and we hope you enjoy your course.

Contents

1 Introducing the qualification

What are Level 3 Technical Occupational Qualifications?

Level 3 Technical Occupational Qualifications are qualifications that are at Level 3 on the Regulated Qualifications Framework (RQF) and are designed to deliver the skills needed to enter or progress in the workplace. They can be delivered through a combination of classroom and work-based learning and assessment.

These qualifications are based on occupational standards designed by employers and published by the Institute for Apprenticeships and Technical Education (IfATE), who also approve the qualifications. IfATE has specified different categories under which Level 3 Technical Qualifications can be approved based on their scope and purpose. Detailed information about these categories can be found on IfATE's website.

Qualification purpose

Pearson BTEC Level 3 Technical Occupational Entry for Cyber Security Technician (Diploma) enables students to develop a purposeful combination of knowledge, skills and behaviours to enter employment as a cyber security technician and provides a strong foundation for them to achieve full occupational competence with further training and development in the workplace.

The qualification, which is mapped to the Cyber Security Technician occupational standard, is designed to meet the needs of adult students (19+) and provides a clear line of sight to employment in an occupation that is recognised and demanded by employers.

The qualification aims to:

- develop students' ability and confidence to apply the knowledge, skills and behaviours when carrying out the occupational duties and functions of a cyber security technician and meet entry level competence
- develop transferable skills and professional behaviours such as managing own time to meet deadlines, managing stakeholder expectations, having a structured approach to prioritising tasks, and reviewing own development needs to keep up to date with evolution in technologies, trends and innovations that are essential to personal effectiveness in a cyber security role
- develop knowledge and understanding of best practices relating to cyber security compliance and compliance monitoring, cyber security audit requirements, procedures and plans, importance of maintaining privacy and confidentiality of information, and the impact of a poor security culture that are important for regulatory compliance and meeting professional requirements in the cyber security sector

- provide opportunities for students to achieve a nationally recognised occupational qualification to support them in taking the next step in their career journey
- provide employers with reliable evidence of students' attainment against the Cyber Security Technician occupational standard and their readiness to enter employment in this sector.

The qualification can be taken on a part time or full-time basis to meet the needs of adult students.

Employer engagement and validation

In developing the Pearson BTEC Level 3 Technical Occupational Entry for Cyber Technician (Diploma), we have worked closely with a dedicated panel of cyber security employers from a range of different types of organisations, who have:

- validated the demand for the qualification and confirmed that it is occupationally relevant and meets the current and emerging needs of industry
- confirmed that students will have an appropriate combination of knowledge, skills, and behaviours relevant to the occupational standard that attests to their readiness to enter into employment in the related occupation.

Progression opportunities

Students who achieve the Pearson BTEC Level 3 Technical Occupational Entry for Cyber Security Technician (Diploma) can progress to roles such as cyber security technologist or cyber security engineer.

2 Qualification summary and key information

Qualification title	Pearson BTEC Level 3 Technical Occupational Entry for Cyber Security Technician (Diploma)
Qualification Number (QN)	610/3933/0
Regulation start date	14/03/2024
Operational start date	01/08/2025
Approved age ranges	19+
Total Qualification Time (TQT)	383
Guided learning hours (GLH)	295
Assessment	Internal assessment.
Grading information	The units within the qualification are graded Pass/Fail. To achieve a Pass, students must achieve a Pass in all three units.
Entry requirements	No prior knowledge, understanding, skills or qualifications are required before students register for this qualification.
Funding	This qualification is eligible for 19+ funding as a Technical Occupational Entry qualification. Information about funding can be found on the Find a learning aim database.
Delivery	This qualifications is designed to be delivered in post 16 learning contexts. Delivery should focus on student's ability to use knowledge, skills and appropriate behaviours in, or to progress to, the workplace. Links with the workplace should be encouraged throughout.

3 Qualification structure

Pearson BTEC Level 3 Technical Occupational Entry for Cyber Security Technician (Diploma)

The requirements outlined in the table below must be met for Pearson to award the qualification.

Minimum number of units that must be achieved	3

Unit number	Mandatory units	Level	Guided learning hours
1	Technologies, Principles and Evolving Threats	3	85
2	Policies and Procedures in Cyber Security	3	50
3	Cryptography and Incident Management	3	160

4 Assessment requirements

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

Units	Assessment methods
All units	Authorised Assignment Briefs are provided for centres to use or adapt. Centres are free to create their own assignment briefs.

Language of assessment

Students must use English only during the assessment of this qualification.

A student taking the qualification(s) may be assessed in British Sign Language where it is permitted for the purposes of reasonable adjustment.

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

Internal assessment

Internally assessed units are subject to standards verification. This means that centres set and mark the final summative assessment for each unit, using the examples and support that Pearson provides.

To pass each internally assessed unit, students 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.

Centres must ensure:

- assessment is carried out by assessors with relevant expertise in both the occupational area and assessment. For the occupational area, this can be evidenced by a relevant qualification or current (within three years) occupational experience that is at an equivalent level or higher than this qualification. Assessment expertise can be evidenced by qualification in teaching or assessing and/or internal quality assurance or current (within three years) experience of assessing or internal verification
- internal verification systems are in place to ensure the quality and authenticity of students' work, as well as the accuracy and consistency of assessment.

Students who do not successfully pass an assignment are allowed to resubmit evidence for the assignment or to retake another assignment.

Levels of control in internal assessment

Task setting

Centres are able to design tasks that address the assessment criteria within a unit. Restrictions on task setting such as mandatory forms of evidence requirement, or restrictions surrounding the context of assessment will be stated within the qualification unit and any accompanying authorised assignment brief(s). Although task setting is characterised as low control, Pearson applies quality assurance methodology to ensure that centre systems are in place to develop and assure high quality assessments for students. The authorised assignment brief serves as a model for the expected presentation of a unit assessment. Further guidance and references are provided in *Section 9: Quality Assurance of centres*.

Task taking

Centres must be able to authenticate the student response to the assessment. Supervision may not always be appropriate, if for example a student is gathering evidence for an assessment that is then prepared in a classroom environment. However, centres must be assured that students produce their own response to assessment criteria. This may require supervision of students in writing up outcomes to ensure they do not use text generative AI software.

Task marking

Centre assessors and tutors will mark the student assessment response, using Pearson BTEC assessment/grading criteria and the guidance we provide in the specification and surrounding process, and training we provide supporting our quality assurance process. Pearson will quality assure the processes that centres use to ensure the standard of marking outcome. We operate a risk-based quality assurance process ensuring that new centres, centres with large cohorts and centres with other risk factors get the support they need to ensure students achieve the outcome they have worked for.

Mandatory evidence for assessment

Units will include information on the mandated types, quality and standard of evidence that students must produce to achieve a unit.

Tutors must ensure that collated tasks/assignments enable students to generate the evidence needed against the assessment criterion standard.

Authorised Assessment Briefs (AABs)

Each unit will have an Authorised Assessment Brief (AAB). The AABs are there to provide an example of what the assessment could look like in terms of the feel, level of demand and integration of mandated evidence required of the assessment. Centres can use the AAB as provided by Pearson. Alternatively, centres may amend the AAB or create their own assignment if they are confident it enables learners to provide suitable and sufficient evidence to meet the stated standard of the assessment criteria and achieve the learning outcomes. Centres are reminded that the AABs form a basis of standardisation of task setting within the Pearson quality assurance process.

A copy of each of these assessments can be downloaded from the qualification page on our website.

5 Centre recognition and approval

Centres must have approval prior to delivering any of the units in this qualification.

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

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.

Centre resource requirements

As part of the approval process, centres must make sure that the resource requirements below are in place before offering the qualification:

- appropriate physical resources (for example, IT, learning materials, teaching rooms) to support the delivery and assessment of the qualification
- suitable staff for delivering and assessing the qualification (see *Section 4 Assessment requirements*)
- systems to ensure continuing professional development (CPD) for staff delivering and assessing the qualification
- health and safety policies that relate to the use of equipment by students
- internal verification systems and procedures (see *Section 4 Assessment requirements*)
- any unit-specific resources stated in individual units.

6 Access to qualifications

Access to qualifications for students with disabilities or specific needs

Equality and fairness are central to our work. Our *Equality, diversity and inclusion policy* requires all students to have equal opportunity to access our qualifications and assessments, and that our qualifications are awarded in a way that is fair to every student.

We are committed to making sure that:

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

For students with disabilities and specific needs, the 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.

Centres must deliver the qualification in accordance with current equality legislation. For full details of the Equality Act 2010, please visit www.legislation.gov.uk.

Reasonable adjustments and special consideration

Centres are permitted to make adjustments to assessment to take account of the needs of individual students. Any reasonable adjustment must reflect the normal learning or working practice of a student in a centre or a student working in the occupational area.

Centres cannot apply their own special consideration – applications for special consideration must be made to Pearson and can be made on a case-by-case basis only.

Centres must follow the guidance in the Pearson document *Guidance for reasonable adjustments and special consideration in vocational internally assessed units*.

7 Recognising prior learning and achievement

Recognition of Prior Learning (RPL) considers whether a student can demonstrate that they can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess and so do not need to develop through a course of learning.

Pearson encourages centres to recognise students' previous achievements and experiences in and outside the workplace, as well as in the classroom. RPL provides a route for the recognition of the achievements resulting from continuous learning.

RPL enables recognition of achievement from a range of activities using any valid assessment methodology. If the assessment requirements of a given unit or qualification have been met, the use of RPL is acceptable for accrediting a unit, units, or a whole qualification. Evidence of learning must be sufficient, reliable and valid.

Further guidance is available in our policy document *Recognition of prior learning policy and process*, available on our website.

8 Quality assurance of centres

For the qualification in this specification, the Pearson quality assurance model will consist of the following processes.

Centres will receive at least one visit from our Standards Verifier, followed by ongoing support and development. This may result in more visits or remote support, as required to complete standards verification. The exact frequency and duration of Standards Verifier visits/remote sampling will reflect the level of risk associated with a programme, taking account of the:

- number of assessment sites
- number and throughput of students
- number and turnover of assessors
- number and turnover of internal verifiers
- amount of previous experience of delivery.

Following registration, centres will be given further quality assurance and sampling guidance.

For further details, please see the work-based learning quality assurance handbooks, available in the support section of our website:

- *Pearson Work-based Learning Centre Guide to Quality Assurance*
- *Pearson Work-based Learning Delivery Guidance & Quality Assurance Requirements.*
- Support is also available on our work based learning quality assurance webpages Quality Assurance – Work-based Learning (WBL) | Pearson qualifications

9 Units

This section of the specification contains the unit that forms the assessment for the qualification.

It is compulsory for students to meet all learning outcomes and the assessment criteria to achieve a grade. The assessment criteria determine the standard required. Content is compulsory unless it is provided as an example and is therefore marked 'e.g.,'. All compulsory content must be delivered, but assessments may not cover all content.

Where legislation is included in delivery and assessment, centres must ensure that it is current and up to date.

Unit 1: Technologies, Principles and Evolving Threats

Level: 3

Guided learning hours: 85

Unit introduction

This unit covers cyber security threats and vulnerabilities, and the methods used to protect systems against threats, including new and evolving cyber security threats. Students will research and examine the many different, new and evolving types of cyber security attacks and novel developments of older ones.

Students will examine the many different types of networks that can be affected by cyber security attacks, the vulnerabilities that exist in networked systems, and the techniques that can be used to defend an organisation's networked systems against new attacks. Students will have the opportunity to use vulnerability assessment tools and different security measures in given scenarios.

Learning outcomes and assessment criteria

To pass this unit, students need 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 a range of network types, software components and common vulnerability exposures	1.1 Analyse categories of cyber security vulnerabilities and common vulnerability exposures and impact on organisations 1.2 Evaluate the uses of network components and related cyber security vulnerabilities 1.3 Complete an outline vulnerability assessment for a given scenario and provide recommendations
2. Understand threats to hardware, software and data, and the impact of these threats on organisations	2.1 Categorise threats, vulnerabilities and risks in preparation for response or escalation 2.2 Evaluate existing and novel cyber security threats and the impact that these threats have on an organisation in a given scenario 2.3 Analyse the use of network reconnaissance techniques in different situations

Learning outcomes	Assessment criteria
3. Understand vulnerabilities of IT systems and processes and use vulnerability tools in vulnerability identification and mitigation	3.1 Analyse vulnerabilities of IT systems and software and the impact these vulnerabilities might have on an organisation 3.2 Analyse vulnerabilities for a given system or scenario and produce a mitigation plan 3.3 Use vulnerability assessment tools in vulnerability identification and mitigation
4. Use hardware-based security measures for IT systems and data	4.1 Use hardware-based security measures for a given system or scenario and produce a security plan 4.2 Use general security measures for a given system or scenario and produce a security plan
5. Use software-based security measures for IT systems and data	5.1 Use software-based security measures for a given system or scenario to produce a security plan 5.2 Use methods for the secure storage, tracking and disposal of different types of digital assets
6. Understand new and current evolving threats in the digital world	6.1 Analyse evolving cyber security issues in the digital world and the impacts for a given scenario, taking into account the sources of verified information and data 6.2 Carry out routine threat intelligence-gathering tasks for a given scenario using external sources
7. Understand how a threat evolves over time and new areas of concern	7.1 Assess how a threat evolves over time and new areas of concern 7.2 Identify and categorise threats, vulnerabilities and risks in preparation for response or escalation 7.3 Present information on how different cyber threats change over time

Unit content

What needs to be learned
Learning outcome 1: Understand a range of network types, software components and common vulnerability exposures
Applications and features of networks Research the uses of a range of network types and related security issues · Network types: o local area network (LAN) o wireless local area network (WLAN) o virtual local area network (VLAN) o metropolitan area network (MAN) o wide area network (WAN) o storage area network (SAN) o personal area network (PAN) o content delivery network (CDN) o virtual private network (VPN) o enterprise private network (EPN) o intranet and extranet o cloud network. · Network topologies: o physical topologies (bus, mesh, ring, star, tree, ad-hoc, hybrid) o logical topologies (bus, ring). · Wired and wireless integration, ethernet standards for wired and wireless (802 family). · Network architectures: o peer-to-peer (structured, unstructured) o client/server (thin client, thick client) o hybrid o remote access network (walled garden, zero trust). · Modern trends – applications, features and security issues: o virtualisation o cloud computing

What needs to be learned

- bring your own device (BYOD)
- software-defined networking (SDN)
- storage-defined networks and the Internet of Things (IoT)
- remote working.

· Applications and features of network hardware components

· Research the uses of a range of network hardware components, and related security issues

· End-user devices:

- personal computer (PC)
- server (application, database, domain name service (DNS), Dynamic Host Communication Protocol (DHCP), file, File Transfer Protocol (FTP), mail, media, print
- proxy, virtual machine, web
- laptop, notebook/netbook
- tablet (slate, convertible, foldable/booklet)
- smartphone
- wearable computer/smart device, including (headset/earbud, watch, wrist computer, clothing and patches, implants, smart glasses/augmented reality display)
- point of sale (POS), card reader/scanner.

· Networked peripheral devices:

- network printers, scanners, photocopiers and multifunction devices
- access controllers (door and lift controls)
- cameras and microphones.

· Network connectivity devices:

- switch (managed, unmanaged, smart/intelligent, modular)
- router (wired, wireless, edge, core, internet/broadband router-modem)
- wireless access point (WAP) (stand-alone, multifunction, controlled/client)
- modem (integrated, stand-alone).
- bridge (simple, multiport, wireless)
- gateway (bi-direction, uni-direction).

What needs to be learned

- Network connection media:
  - cable (twisted pair, coaxial)
  - wireless/radio frequency (wi-fi, Bluetooth, mobile/cellular communication
  - optical fibre
  - light (Li-Fi, infrared (IR)).
- External media and storage:
  - Universal serial bus (USB) drive
  - memory card
  - portable hard drive (solid state device (SSD), magnetic disk).
- Application and features of network software components
- Research the uses of a range of network software components, and related security issues
- Operating systems:
  - network (MS Windows, Unix and Unix-like, Linux)
  - end-user device (Android, Apple iOS, Linux, MS Windows, ChromeOS)
  - for devices such as routers and switches (open source, e.g. OpenWrt, propriatory, e.g. Cisco IOS).
- Network monitoring, management and troubleshooting tools:
  - remote access/administration tool Remote Server Administration Tools (RSAT) (Windows), Remote Console/GUI Management Tool (Linux/Unix), Remote Desktop Manager)
  - performance monitor (Windows), TOP and TOP variants (Linux)
  - event viewer (Windows), read /var/log (Linux cmd line), system log viewer (Linux GUI)
  - vulnerability scanner
  - packet sniffer/packet analyser/protocol analyser/network analyser
  - ping, trace and network discovery.
- Network applications:
  - remote working tools (video conference, chat, online applications, browser, shared file management, shared file storage, remote desktop)
  - database
  - document manager.

What needs to be learned
Learning outcome 2: Understand threats to hardware, software and data, and the impact these threats have on organisations
Threat sources and threat identification Research existing cyber security threats · Understand, identify and categorise threats: o malware (viruses, spyware, adware) o denial of service (DoS) and distributed denial of service (DDoS) o hacking, unauthorised access o social engineering attacks o insider threats o zero-day vulnerabilities o eavesdropping o interception and replay o ARP spoofing o DNS poisoning o man-in-the-middle o crypto-jacking o buffer overflow o Structured Query Language (SQL) injection o suspicious user behaviour o suspicious device behaviour o unauthorised system changes. · Monitor, detect and escalate potential threats: o threat signatures o behaviour analytics o intruder traps o reporting and escalation procedures and logs. Evolving cyber security issues Research novel cyber security threats, including changes in existing threats · Threats to: o critical infrastructure

What needs to be learned
o national assets o communication systems o control systems. · The Internet of Things (IoT): o rogue devices o vehicles and robotic systems o privacy, eavesdropping, data harvesting via IoT devices o weak built-in security o Use of IoT devices as an attack surface for wider systems. · Use of artificial intelligence (AI): o AI threat hunters, false positives and negatives o AI used for developing and testing malware, phishing, deep fakes o poisoning of data sets, generating false data.
Learning outcome 3: Understand vulnerabilities of IT systems and processes and use vulnerability tools in vulnerability identification and mitigation
Vulnerability categories Research vulnerabilities of IT systems and software · Understand types of vulnerability: o network vulnerabilities o operating system vulnerabilities o process (or procedural) vulnerabilities o human vulnerabilities. · Identify and categorise vulnerabilities: o missing or weak encryption o weak/missing access control o unrestricted upload/download of files o code download/run without integrity/hash checks o URL redirection/cross-site scripting o weak/unchanged/stolen/compromised passwords/user credentials o websites using Secure Sockets Layer (SSL) instead of Transport Layer Security (TLS)

What needs to be learned
o lack of physical security measures o unsecured application programming interface (API) o outdated/unpatched software. Vulnerability assessment Research vulnerabilities for a given system or scenario and produce a mitigation plan · Understand the components of a vulnerability assessment: o identification o analysis o assess risk level o close security gaps o reporting and documentation. · Understand the types of vulnerability assessment: o network-based o wireless network-based o application-based o API-based o host/device-based o cloud-based o social engineering-based o physical vulnerability. · Evaluate the results of a vulnerability assessment and its impact on an organisation. · Provide evidence-based recommendations. Vulnerability assessment tools Research and use vulnerability assessment tools and understand their role in vulnerability identification and mitigation · Understand common vulnerability assessment tools: o network mapping o protocol analysis o traffic capture o permissions and access level scanners o patch numbers/software version logging

What needs to be learned
o configuration settings scanners o database architecture and interface scanners o website structure and scripting scanners.
Learning outcome 4: Use hardware-based security measures for IT systems and data
Hardware-based security measures Research and use hardware-based security measures for a given system or scenario and produce a security plan · Hardware security modules (HSMs): o certification o use cases o forms – cards, external devices, HSM as a service o trusted platform module (TPM). · Supply chain trust and security, vendors and other suppliers: o understanding risks, supplier's protection, supplier's chain, subcontractors o chain control, minimum standards, up-chain responsibilities o checks and audits. · Firmware updates: o logging and monitoring version numbers o automated/scheduled updates o pre-rollout testing of updates o cryptographic signatures. · Hardware upgrades: o old/legacy/out-of-support hardware as an attack surface o improvements to security features on latest hardware. o General security measures Research and use general security measures for a given system or scenario and produce a security plan · Physical access controls and monitoring of secure areas: o locks – electronic, mechanical, hybrid o surveillance, cameras, infrared/motion detectors

What needs to be learned
o access control methods, Radio Frequency Identification (RFID), Bluetooth, Near Field Communication (NFC), biometrics, PIN, QR code, microchip card. · Hardware audits: o labelling, logging o identifying maintenance/replacement requirements o checks location and security of data storage devices o reveals potential security issues. · Anti-theft measures and anti-tamper housings: o tags, smart and dumb o chemical markers o hidden physical markers, microdots, RFID chips o tracking devices and software o remote wipe/locking system o locks, cables, cages and mountings.
Learning outcome 5: Use software-based security measures for IT systems and data
Administrative operational tasks Research and use software security measures for a given system or scenario and produce a security plan · Common security administrative operational tasks. · Configuring security systems. · Monitoring network traffic. · Creating network policies. · Overseeing authorisation and access. · Analysing security requirements and making recommendations. · Maintaining logs and records. · Managing patches and updates. · Digital information assets. · Understand types of digital information assets: 1. documents 2. images

What needs to be learned
3. data 4. video and audio 5. code 6. cryptocurrency 7. account information. · Inventory and tracking of information assets: o version controls o data catalogue/dictionary o locking assets/setting permissions o licences. · Secure information asset disposal: o data protection legislation requirements o inventory update o deletion versus archiving o secure deletion algorithms, US Department of Defense (DoD 5220.22-M), the Peter Gutmann algorithm, 3 Pass British HMG IS5 o physical destruction of storage media.
Learning outcome 6: Understand new and current evolving threats in the digital world
Information sources Research up-to-date information on cyber threats · National Cyber Security Centre (NCSC) UK: o guides for cyber security professionals o latest threat reports and malware analysis o incident reporting o news (reports and advisories on recent activity). · National Institute of Standards and Technology (NIST) USA: o news (reports and advisories on recent activity). · European Union Agency for Cybersecurity (ENISA) EU: o online security assessment tools o news (reports and advisories on recent activity).

What needs to be learned
· Center for Internet Security (CIS) USA and worldwide: o critical security controls o benchmarks. · Open Web Application Security Project (OWASP) worldwide: o OWASP Top 10 o information sheets on prevention measures.
Learning outcome 7: Understand how a threat evolves over time and new areas of concern
Evolving threats Research up-to-date information on how different cyber threats change over time · Social engineering: o spear-phishing o whaling o smishing o vishing o business email attacks o crypto-scams. · Cryptographic failures: o continued use of older/deprecated protocols, keys, hash functions o unvalidated or expired certificates o failure to enforce encryption, using HTTP, SMTP, FTP. · Ransomware: o rise of Ransomware as a Service (RaaS) o modernised toolkit by high level threat actors. · Cloud vulnerabilities: o web app breaches. · End-user devices: o issues with flexible/remote/home working using non-organisation devices o targeting of mobile device management systems.

What needs to be learned

- Data breaches:
  - issues with exponential increase of data being moved/stored
  - cascade/spiderweb effect, one breach providing data for attacking other data stores.
- Nation state activity:
  - state sponsored hacktivists or terrorists supporting a nation/cause
  - cyber warfare
  - cyber-enabled espionage
  - hack and leak of compromising material
  - cyber destruction of systems and institutions
  - cyber theft of intellectual property (IP)
  - insertion of exploits into supply chain (eavesdropping, back doors)
  - internet disruption attempts.
- Zero-day exploits:
  - new areas of concern
  - research up-to-date information on novel cyber threats or novel applications of older threats.
- Automotive hacking:
  - taking over control
  - eavesdropping on occupants
  - disabling vehicles.
- Automated machinery hacking:
  - disabling/destruction of machinery
  - sabotage (setting bad parameters, causing malfunctions affecting output).
- Artificial intelligence (AI):
  - use of AI to write malware
  - use of AI to mount attacks (DDoS, data poisoning, creating fakes for social engineering, and disinformation campaigns).
- 5G networks:
  - danger to mission-critical applications such as emergency response
  - attacks when sharing, switching and slicing networks
  - supply chain security issues.

What needs to be learned
· IoT networks: o IoT devices made with weak/no security built in o supply chain security issues o default mode of unencrypted traffic o use in botnets o non-traditional devices/connections as point of entry to networks o privacy issues (eavesdropping, data harvesting via IoT devices).

Essential information for tutors and assessors

Essential resources

For this unit, students will need access to computer facilities and the internet. Students must also have access to the use of Cisco labs/Pearson Academy facilities for practical work.

Assessment

This unit is internally assessed. To pass this unit, the evidence that students present for assessment must demonstrate that they have met the required standard specified in the learning outcomes and assessment criteria.

The assessment for this unit should be set in the context of students showing how they have demonstrated and developed their skills, drawing on learning from the unit. It must be designed in a way that enables students to meet all the assessment criteria.

The Authorised Assignment Brief (AAB) that includes this unit is a recommended assessment approach and sets out suitable sources of evidence for the learning outcomes. It also gives information about the standard and quality of evidence expected for students to achieve the learning outcome and pass each assignment. It is important that the information is used carefully alongside the assessment criteria.

Centres are free to amend the AAB or create their own assignment if they are confident it enables students to provide suitable and sufficient evidence to meet the stated standard of the assessment criteria and achieve the learning outcomes.

Unit 2: Policies and Procedures in Cyber Security

Level: 3

Guided learning hours: 50

Unit introduction

This unit covers the structure and cyber security related processes of organisations. Students will examine different types of organisations and look at cyber security processes and career paths within them.

This unit introduces students to the UK, EU and international legislation that applies to cyber security issues. Students will examine different cyber security policies and standards and how they can be used to mitigate cyber security threats to an organisation. They will also have the opportunity to produce and amend policies and standards for given scenarios.

In the final part of the unit students will look at how the role of cyber security technician fits into the wider digital landscape and how multidisciplinary teams link with other areas of an organisation.

Learning outcomes and assessment criteria

To pass this unit, students need 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 current UK, EU and international legislation that applies to cyber security issues	1.1 Summarise UK legislation, its scope and its enforcement 1.2 Summarise EU and appropriate other international legislation, its scope and its enforcement

Learning outcomes	Assessment criteria
2. Understand cyber security related policies and produce policies appropriate for a given scenario	2.2 Explain cyber security policies and relationship to an information security management system (ISMS) 2.3 Explain how current legislation relates to or impacts on an organisation's policies 2.4 Analyse the components of an effective security culture and the impact of a poor security culture 2.5 Produce cyber security related policies appropriate for an organisation in a given scenario, taking account of risk assessment and management, business impact analysis principles and appropriate cyber security compliance 2.6 Monitor and amend cyber security related policies using compliance monitoring techniques
3. Understand internal and external cyber security standards and produce security standards appropriate for a given scenario	3.1 Explain cyber security standards based on an information security management system (ISMS) 3.2 Explain how current legislation relates to or impacts on internal and external cyber security standards 3.3 Produce cyber security related standards appropriate for a given scenario, taking into account the ethical use of data
4. Understand organisational structure and team and individual roles related to cyber security	4.1 Assess organisational structures within cyber security 4.2 Explain how the role of cyber security technician fits into the wider digital landscape and any current or future regulatory requirements 4.3 Discuss roles within a multidisciplinary team and the interfaces with other areas of an organisation
5. Understand career paths and teamworking in cyber security	5.1 Discuss career paths and job roles within cyber security 5.2 Use communication skills to cooperate as part of a multifunctional, multidisciplinary team to provide an effective interface between internal or external users and suppliers 5.3 Explain cyber security positions and career paths and the factors involved in creating a positive cyber security culture

Unit content

What needs to be learned
Learning outcome 1: Understand current UK, EU and international legislation that applies to cyber security issues
Current legislation relating to cyber security (content below refers to the latest version of each act) Research UK legislation, its scope and enforcement, including the obligations of organisations and cyber security professionals · Data Protection Act – General Data Protection Regulation (GDPR): o Information Commissioner's Office (ICO). · Regulation of Investigatory Powers Act: o amendments and expansions – Investigatory Powers Act, Data Retention and Acquisition Regulations o Investigatory Powers Commissioner's Office (IPCO). · Human Rights Act: o Human Rights Act reform, Bill of Rights. · Computer Misuse Act: o amendments and expansions – Part 5 of the Police and Justice Act, Part 2 of the Serious Crime Act. · Freedom of Information Act. · Official Secrets Act: o amendments and expansions – Official Secrets Act. · Wireless Telegraphy Act: o Office of Communications (Ofcom). EU and international legislation Research EU and appropriate other international legislation, its scope and enforcement, including the obligations of organisations and cyber security professionals · Jurisdiction and cross-border enforcement issues. · General Data Protection Regulation ((EU) 2016/679) (EU GDPR): o extra-territorial effect o adequacy.

What needs to be learned
· Bilateral treaties and frameworks that affect UK organisations. · Nation state efforts to extend and/or police their jurisdiction internationally.
Learning outcome 2: Understand cyber security related policies and produce policies appropriate for a given scenario
· CIA triad (confidentiality, integrity, availability): o for guiding policies o for developing systems and processes. · Enforcing security policies and best practices. · User training policies: o social engineering defence o password generation and management o reporting suspicious activities o acceptable use o bring your own device (BYOD) o data handling o privacy and security. · Risk assessments: o regulatory requirements o legal constraints o external pressures such as customers' demands or public opinion o basic model – identification, assessment, mitigation, prevention. · Cyber security plans – policies, procedures and controls: o for cyber attacks o for data breaches. · Disaster recovery plans – non-cyber security: o prevention o mitigation o preparedness o response o recovery.

What needs to be learned
· Disaster recovery plans – cyber security disaster: o team members o links to non-cyber security disaster processes o business continuity o data protection o minimising losses – financial, reputation, legal consequences o communication – within disaster recovery team, within the organisation, externally o restoration of systems and data analysis and recommendations for improvements. · Asset control and disposal: o inventory control and auditing o tracking o licences. · Cyber security audit requirements: o data security procedures o network access o data encryption and movement o operational security o network monitoring o patching o physical security.
Learning outcome 3: Understand internal and external cyber security standards and produce security standards appropriate for a given scenario
Internal, organisational standards · Ethical use of information assets. · Third party supplier security standards. External standards · UK and appropriate international standards, their scope and enforcement, including the obligations of organisations and cyber security professionals. · Professional body codes of conduct, · Ethical use of information assets.

What needs to be learned
· ISO 27001 (October 2022) information security management. · UK Cyber Security Council code of ethics. · Payment Card Industry Data Security Standard (PCI-DSS). · Standards from organisations such as the National Institute of Standards and Technology (NIST), European Union Agency for Cybersecurity (ENISA), National Cyber Security Centre (NCSC).
Learning outcome 4: Understand organisational structure and team and individual roles related to cyber security
Organisational structure · Characteristics and application of structure types: o functional/departmental o hierarchical o flat o divisional (by market, industry/product, geographical area, function) o matrix o team-based o network-based. · Purposes of organisational structure: o facilitate management and administration o improve stability o improve efficiency o enable clear communications o clearly define roles and responsibilities o facilitate training and development o facilitate effective/optimum use of resources. Organisational control Research organisational management · Characteristics and application of management types: o autocratic o bureaucratic o democratic o paternalistic

What needs to be learned
o free rein or laissez-faire o mentoring. · Purposes of organisational management: o setting and achieving objectives o creating/arranging cooperation and coordination o allocation/conserving of resources o regulating/organising activities o create/maintain functional/friendly relationships (up, down, sideways).
Learning outcome 5: Understand career paths and teamworking in cyber security
Cyber security related career paths. · Common cyber security positions: o Level 0/feeder roles (IT support, software development. networking, systems engineering, financial and planning) o Level 1/entry level (IT security/cyber security specialist, cybercrime/digital forensics analyst, incident response specialist/analyst, IT auditor) o Level 2/mid-level (IT security/cyber security analyst, cyber security consultant, cloud security specialist) o Level 3/high level (certified information security manager/professional, security/cyber security engineer, recovery specialist, security architect). · Role of cyber security professionals in establishing a cyber security culture: o guidance: - National Cyber Security Centre (NCSC) – developing a positive cyber security culture; you shape security - European Union Agency for Network and Information Security (ENISA) – cyber security culture in organisations. o factors in building a culture: - leadership, engagement of management and cyber security professionals at all levels - liaison, between sectors/departments/teams - education/building awareness, in, e.g., management, employees, remote workers, third parties (vendors, customers, visitors) - relevance of cyber security to, e.g., training, work routines, processes

What needs to be learned
- personalisation/tailoring of, e.g., style, content, training methods, reinforcement methods - values and attitudes, e.g. human factors and fallibilities, a learning experience rather than blame games, rewarding success, making security interesting - monitoring and measuring of training results to find, e.g., what methods/materials work, what adds value, what incentivises good culture - the wider world, sharing cyber security information with other organisations – even competitors.

Essential information for tutors and assessors

Essential resources

For this unit, students will need access to computer facilities and the internet. Students must also have access to the use of Cisco labs/Pearson Academy facilities for practical work.

Assessment

This unit is internally assessed. To pass this unit, the evidence that students present for assessment must demonstrate that they have met the required standard specified in the learning outcomes and assessment criteria.

The assessment for this unit should be set in the context of students showing how they have demonstrated and developed their skills, drawing on learning from the unit. It must be designed in a way that enables students to meet all the assessment criteria.

The Authorised Assignment Brief (AAB) that includes this unit is a recommended assessment approach and sets out suitable sources of evidence for the learning outcomes. It also gives information about the standard and quality of evidence expected for students to achieve the learning outcome and pass each assignment. It is important that the information is used carefully alongside the assessment criteria.

Centres are free to amend the AAB or create their own assignment if they are confident it enables students to provide suitable and sufficient evidence to meet the stated standard of the assessment criteria and achieve the learning outcomes.

Unit 3: Cryptography and Incident Management

Level: 3

Guided learning hours: 160

Unit introduction

This unit covers cryptography and access control methods used to protect systems against threats. Students will examine the role of cryptography in protecting data and networked systems through systems and processes used to control access and digital identities. Students will have the opportunity to apply cryptographic systems and processes to secure data.

Students will carry out a risk assessment, interpret information about a security event incident and produce the relevant documentation. Students will use network administration tools and explore exception and management reporting and the requirements for cyber security audit.

Learning outcomes and assessment criteria

To pass this unit, students need 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 incident and event security and management	1.1 Analyse information about a security event incident, exception and management reporting requirements 1.2 Explain how to document incident and event information as part of a chain of evidence
2. Understand use of forensic tools and documentation for a given system or scenario	2.1 Explain computer forensic principles in relation to safeguarding evidence against contamination and being compromised 2.2 Use a range of digital forensic tools suitable for a given system or scenario 2.3 Produce appropriate documents relating to cybersecurity events for a given system or scenario

Learning outcomes	Assessment criteria
3. Understand and apply systems and processes to control access to hardware, software and data	3.1 Explain the principles of identity and access management and the inter-relationship between privacy and access rights and access control 3.2 Analyse the types of access control, access control mechanisms and application control 3.3 Review and modify access rights to digital information systems, services, devices or data for a given scenario
4. Understand and apply systems and processes to establish and control digital identities	4.1 Analyse key protocols, security risks to keys and key management systems 4.2 Explain certificate types and authorities and the use of certificate management tools for a given scenario 4.3 Review and modify access rights to digital information systems, services, devices or data for a given scenario
5. Understand cryptographic systems and processes to secure data	5.1 5.1 Explain and use cyphers to secure data in a given scenario 5.2 Explain and use hash algorithms for moving and resting data in a given scenario
6. Understand organisational cyber security related processes	6.1 Analyse cyber security related processes within organisations, including concepts of service desk delivery and how to respond to requests for assistance received by a service desk 6.2 Explain different methods of escalation and the need to communicate accurately and appropriately during an escalation
7. Understand and apply network infrastructure and resources for a given system or scenario	7.1 Apply network addresses and protocols in the context of network administration and security 7.2 Apply network domains and segments in the context of network administration and security 7.3 Use network infrastructure services in the context of network administration and security

Learning outcomes	Assessment criteria
8. Use network administration tools	8.1 Evaluate system administration tools in the context of network administration and security 8.2 Evaluate third party administration tools in the context of network administration and security 8.3 Use system administration tools in the context of network administration and security 8.4 Use third party administration tools in the context of network administration and security
9. Understand the process of risk assessment and carry out a risk assessment for a given scenario	9.1 Analyse a given scenario for potential disruptions of service and carry out a risk assessment to identify appropriate disaster prevention and recovery methods
10. Understand the process of planning for continuity of service and produce plans for given incidents	10.1 Analyse a given scenario for potential disruptions of service and produce plans for continuity of service for a range of possible incidents 10.2 Use a range of backup and recovery tools suitable for a given scenario
11. Understand exception and management reporting and the requirements for cyber security audit	11.1 Explore the requirements for exception and management reporting, and incident and event information as part of a chain of evidence 11.2 Explore cyber security audit requirements, procedures and plans, and the need to obtain and document evidence in an appropriate form

Unit content

What needs to be learned
Learning outcome 1: Understand incident and event security and management
Research and plan for disruption of service events · Disaster recovery standards: o ISO 22301:2019 – Security and resilience – Business continuity management systems (BCMS) – Requirements o ISO/IEC 27031:2011 – Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity. · Disaster recovery stages: o prevention o preparation/prevention o mitigation o response o recovery. · Disaster types: o natural (flood, fire, extreme weather, disease, earthquake) o technological (system failure, accident, utility failure) o human (cyber attack, sabotage, vandalism) o national (terrorism, civic unrest, cyber warfare).
Learning outcome 2: Understand use of forensic tools and documentation for a given system or scenario
Incident response investigation Research and use a range of digital forensic tools suitable for a given system or scenario · Digital forensics types (network, computer, mobile device, database and other structured data, malware). · Digital forensics processes: o establish and maintain chain of custody o establish legal rights and limitations in examining data/devices o collect/preserve (take control of assets, log/tag/document the assets, prevent data loss or corruption, create copies/images)

What needs to be learned

- examine (preparation of devices/media, extraction of data, identification of relevant material, log/tag/document the process)
- analyse (what the data is, who created/changed it, why, where, when and how)
- report (how the data/analysis relates to the incident, presented in an appropriate format and language)
- keyword search.

· Digital forensics tools (commercial packages and suites, open source, online, offline):

- data/disk imager
- metadata reader/analyser
- RAM capture
- browser analysis (cookies, downloads, history, cache, bookmarks, add-ons and extensions, passwords)
- real time monitoring and reporting (network, device, user, application)
- log reader/analyser.

· Digital forensics techniques:

- data/file recovery (deleted, corrupted, moved, overwritten)
- decryption (hashed data, hidden/steganographic data)
- live/running system (contents of volatile memory – RAM, cache)
- anomaly detection (compare drives/data sets/files with copies held elsewhere)
- stochastic/statistical (looking for patterns in access/activity).

Incident response planning and reporting

Research and produce plans for and reports on cyber security events for a given system or scenario

· Cyber security incident response team (CSIRT) guidance:

- NCSC – Build: A cyber security incident response team (CSIRT)
- National Institute of Standards and Technology (NIST) – Computer Security Incident Handling Guide.

· Cyber security incident response team (CSIRT) structures – varies with organisation size and type:

- core team (e.g. CSIRT leader/incident manager, IT/cyber security staff, senior management, investigators, analysts)
- extended team (e.g. legal, public relations (PR), HR, customer services)

What needs to be learned
o external members (e.g. police, National Cyber Security Centre (NCSC), Information Commissioner's Office (ICO), third party disaster recovery specialists) o CSIRT types (full time, part time, ad-hoc, centralised, by department/location, distributed, third party/outsourced). · CSIRT responsibilities, including: o create/amend incident response plans o categorise security incidents (type, severity) o communicate/meet when notified of an incident o carry out a preliminary assessment (possible cause, type and extent of damage) o activate appropriate/pre-planned response o select/co-opt addition members as needed/planned o supervise/assist with recovery procedures o document and report on the incident.
Learning outcome 3: Understand and apply systems and processes to control access to hardware, software and data
Access management · Access control – types: o mandatory o discretionary o role-based o rule-based o attribute-based o break-glass. · Access control – systems: o human o mechanical locks and keys o electronic locks and readers/scanners (basic, semi-intelligent, intelligent) o biometrics o cards and fobs (Bluetooth, Near Field Communication (NFC), magnetic strip, chip and pin, bar and QR code) o single sign on (SSO) services o mobile devices (used as a card, one-time passwords (OTPs), magic links).

What needs to be learned
· Access control – logical: o authentication factors (knowledge, ownership, inherence) o authentication types (single factor, multifactor, strong, continuous) o authorisation (user/client privileges, access levels) o federation (single sign-on without passwords, user directory, identity providers).
Learning outcome 4: Understand and apply systems and processes to establish and control digital identities
Key management Research key protocols and security risks to keys and use key management systems · Key life cycle: o generation o registration o storage o distribution and installation o rotation o update o backup o recovery. o revocation o suspension o destruction. · Key types (symmetric, asymmetric). · Role segregation (separation of duties, dual control, split knowledge). · Protocols (Public key infrastructure (PKI), Key Management Interoperability Protocol (KMIP)). · Risks: o weak keys o incorrect use o reuse o poor storage o overuse/non-rotation

What needs to be learned
o poor protection o destruction failure o insecure movement o human error o inadequate logging. Certificate types and authorities and use certificate management systems · Certificate life cycle: o discovery o creation or purchase o installation o storage o monitoring o renewal o replacement o revocation. · Certificate managers. · Certificate authorities (internal, external). · Certificate types: o signing (code, document, email) o Transport Layer Security (TLS) and Secure Sockets Layer (SSL) o EU qualified certificates (electronic Identification, Authentication and Trust Services (eIDAS) and UK equivalent (UK eIDAS)) o Internet of Things (IoT) device certificate o Qualified trust service provider (QTSP).

What needs to be learned
Learning outcome 5: Understand cryptographic systems and processes to secure data
Cyphers and hashing · Cypher objectives (confidentiality, non-repudiation, integrity, authenticity). · Cypher types: o substitution o transposition o XOR o steganographic o one time pad. · Symmetric key algorithm, Advanced Encryption Standard (AES). · Asymmetric key algorithm, Rivest-Shamir-Adleman (RSA). Encrypting data Research and use hash algorithms for moving and resting data · Data encryption at rest (full disk encryption, file encryption). · Data encryption when moving (use of VPN and secure communication protocols (IPSec, SSL/TLS)). · Hashing algorithms: o message-digest algorithm (MD5) o Secure Hash Algorithms (SHA-2 and SHA-3) o RIPE Message Digest (RIPEMD) o Whirlpool o ISO/IEC 10118-3:2018 o salting. · Hashing attacks: o collision o pre-image o birthday o length extension o rainbow table.

What needs to be learned
Learning outcome 6: Understand organisational cyber security related processes
Cyber security related processes within organisations · Cyber security process types: o management systems, ISO/IEC 27000 family o policies o procedures/regular tasks o audits o governance o control o penetration testing. · Documenting a process: o identify, name and describe the process o define the scope/boundaries o identify the expected outputs o detail the expected inputs and required resources o walk through the process in a logical sequence to check completeness/workability o decide people/roles to carry out the process o produce a visual representation of the process (flowchart, workflow diagram) o review, test and amend. · Technical support process for cyber security incidents: o opening ticket/collecting information o triage/assessing importance o allocation of resources/cyber security personnel o escalation – to next level of support o resolution and recording o documentation and reporting.

What needs to be learned

Learning outcome 7: Understand and apply network infrastructure and resources for a given system or scenario

Addresses and protocols

- Transmission Control Protocol/Internet Protocol (TCP/IP):
  - five layer model, layers and functions
  - User Datagram Protocol (UDP)
  - common TCP/IP port numbers and uses
  - packets, packet headers and encapsulation.
- Seven layer open systems interconnection (OSI) model:
  - layers and functions
  - relationship to TCP/IP.
- Network address translation (NAT) (static, dynamic):
  - packet header editing.
- IPv4 and IPv6 addressing.
- Request for Comments (RFC) 1918 private address ranges.

Domains and segmentation

- Application of domains, sub-domains and segmentation:
  - Active Directory (AD), Lightweight Directory Access Protocol (LDAP)
  - Trust relationships
  - Kerberos
  - ISO/IEC 27002:2022.
- Application of network devices to configure networks:
  - domain controller
  - Dynamic Host Communication Protocol (DHCP) server
  - router
  - managed switch
  - bridge.

Network infrastructure services

- Application and function of network infrastructure services and resources:
  - Domain Name System (DNS)
  - directory services (Active Directory, open directory, OpenLDAP)

What needs to be learned
o authentication services o Dynamic Host Configuration Protocol (DHCP) o routing o remote access services o file and print services o web, mail and communications services.
Learning outcome 8: Use network administration tools
Operating system administration tools Research and use system administration tools in the context of network administration and security · Group and local security policy, · User/profile/account management. · Scheduling. · Backup and recovery (file level, system level). Third party administration tools Research and use third party administration tools in the context of network administration and security · Patch management. · Licence management. · Log analysis. · Network mapping. · Application monitoring.
Learning outcome 9: Understand the process of risk assessment and carry out a risk assessment for a given scenario
Analyse the cyber security aspects of a given scenario and perform a risk assessment · Risk assessment standards, guidance and templates: o ISO/IEC 27001:2022 – standard for information security management systems (ISMS) o National Cyber Security Centre (NCSC) – risk management guidance o Health and Safety Executive (HSE) – managing risks and risk assessment at work.

What needs to be learned
· Risk assessment stages: o identify threats, vulnerabilities, hazards o assess the likelihood and impact of each risk o evaluate possible responses/select the best/most appropriate one o recording and reporting o monitor and review. · Risk assessment methodologies: o asset-based/component-based – threats to digital assets and their storage locations o scenario-based – looking at security incidents that might occur o system-based – a top-down approach looking at interactions between parts of the system, including people. · Compliance: o legal, regulatory, contractual obligations o risk management versus compliance. · Prioritisation: o by levels (severity x probability) o by weighted levels, allowing for, e.g., costs, time, technical requirements o by organisational priority, e.g. human safety (customer, visitor, worker), commercial value/cost (process revenue, cost of safety measures, ease of restore/reset), image/public relations (impact on confidence/company value, loss of business).
Learning outcome 10: Understand the process of planning for continuity of service and produce plans for given incidents
Disaster recovery planning Research scenarios for potential disruptions of service and produce plans for continuity of service for a range of possible incidents · Planning stages: o create a planning team (IT specialists, management, human resources (HR), maintenance and utilities, department representatives) o establish and maintain a list of names and emergency contact methods for everyone in the organisation

What needs to be learned
o establish a chain of command, with alternatives/deputies o create plans, alternative plans and fallback positions for possible scenarios o use the risk assessments to check coverage of possible scenarios o test and revise the plans. Backup and recovery Research and use a range of backup and recovery tools suitable for a given scenario · Disaster recovery methods: o data backup (on-site, off-site, on removable media, backup as a service) o backup types (full, differential, incremental) o data and infrastructure backup (cold site, hot site, using virtual machines) o disaster recovery as a service. · Disaster recovery tools: o data replication tools for (data, files, disk images, virtual machine images) o data compression tools o backup tools (automated, manual) o data and system restoration tools o remote working and administration tools o system checking and cleaning tools following cyber attacks. · Restoration considerations: o objectives and time scheduling o order of priority for systems and data o communications (public/customer relations and within the organisation) o legal, regulatory, contractual obligations o testing, reporting and revising disaster recovery plans.
Learning outcome 11: Understand exception and management reporting and the requirements for cyber security audit
Incident response planning and reporting Research and produce plans for and reports on cyber security events for a given system or scenario · Cyber security incident response team (CSIRT) guidance: o National Cyber Security Centre (NCSC) – Build: A cyber security incident response team (CSIRT)

What needs to be learned

- National Institute of Standards and Technology (NIST) – Computer Security Incident Handling Guide.

- Cyber security incident response team (CSIRT) structures – varies with organisation size and type:
  - core team (e.g. CSIRT leader/incident manager, IT/cyber security staff, senior management, investigators, analysts)
  - extended team (e.g. legal, public relations (PR), human resources (HR), customer services)
  - external members (e.g. police, National Cyber Security Centre (NCSC), Information Commissioner's Office (ICO), third party disaster recovery specialists)
  - CSIRT types (full time, part time, ad-hoc, centralised, by department/location, distributed, third party/outsourced).
- CSIRT responsibilities, including:
  - create/amend incident response plans
  - categorise security incidents (type, severity)
  - communicate/meet when notified of an incident
  - carry out a preliminary assessment (possible cause, type and extent of damage)
  - activate appropriate/pre-planned response
  - select/co-opt addition members as needed/planned
  - supervise/assist with recovery procedures
  - document and report on the incident.

Essential information for tutors and assessors

Essential resources

For this unit, students will need access to computer facilities and the internet. Students must also have access to the use of Cisco labs/Pearson Academy facilities for practical work.

Assessment

This unit is internally assessed. To pass this unit, the evidence that students present for assessment must demonstrate that they have met the required standard specified in the learning outcomes and assessment criteria.

The assessment for this unit should be set in the context of the students showing how they have demonstrated and developed their skills, drawing on learning from the unit. It must be designed in a way that enables students to meet all the assessment criteria.

The Authorised Assignment Brief (AAB) that includes this unit is a recommended assessment approach and sets out suitable sources of evidence for the learning outcomes. It also gives information about the standard and quality of evidence expected for students to achieve the learning outcome and pass each assignment. It is important that the information is used carefully alongside the assessment criteria.

Centres are free to amend the AAB or create their own assignment if they are confident it enables students to provide suitable and sufficient evidence to meet the stated standard of the assessment criteria and achieve the learning outcomes.

10 Appeals

Centres must have a policy for dealing with appeals from students. Appeals may relate to assessment decisions being incorrect or assessment not being conducted fairly. The first step in such a policy is a consideration of the evidence by a lead internal verifier or other member of the programme team. The assessment plan should allow time for potential appeals after students have been given assessment decisions.

Centres must document all students' appeals and their resolutions. Further information on the appeals process can be found in the document *Internal assessment in vocational qualifications: Reviews and appeals policy*, available on our website.

11 Malpractice

Dealing with malpractice in assessment

Malpractice refers to 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 actions of malpractice by students, centre staff or centres in connection with Pearson qualifications. Pearson may impose penalties and/or sanctions on students, 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 students, please see Pearson's *Centre Guidance: Dealing with Malpractice* available on our website.

Centres are required to take steps to prevent malpractice and to investigate instances of suspected malpractice. Students must be given information that explains what malpractice is for internal assessment and how suspected incidents will be dealt with by the centre. The *Centre Guidance: Dealing with Malpractice* document gives full information on the actions we expect you to take.

Pearson may conduct investigations if we believe a centre is failing to conduct internal assessment according to our policies. The above document gives further information and examples. It details the penalties and sanctions that may be imposed.

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

Student malpractice

The head of centre is required to report incidents of suspected student malpractice that occur during Pearson qualifications. We ask centres to complete *JCQ Form M1* (www.jcq.org.uk/malpractice) and email it with any accompanying documents (signed statements from the student, 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 students lies with Pearson.

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

Failure to report malpractice constitutes staff or centre malpractice.

Tutor/centre malpractice

The head of centre is required to inform Pearson's Investigations team of any incident of suspected malpractice (which includes maladministration) by centre staff before any investigation is undertaken. The head of centre is requested to inform the Investigations team by submitting a *JCQ M2* 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.

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.

You should be aware that Pearson may need to suspend 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, 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:

- requiring centres to create an improvement action plan
- requiring staff members to receive further training
- placing temporary suspensions on certification of students
- placing temporary suspensions on registration of students
- 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 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 students 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 the *JCQ Appeals booklet* (www.jcq.org.uk/exams-office/appeals).

12 Further information and publications

- Edexcel, BTEC and Pearson Work Based Learning contact details: https://qualifications.pearson.com/en/contact-us.html.
- Books, software and online resources for UK schools and colleges: www.pearsonschoolsandfecolleges.co.uk.
- Our publications catalogue lists all the material available to support our qualifications. To access the catalogue and order publications, please visit our website.

Further documents that support the information in this specification:

- *Access arrangements and reasonable adjustments and special consideration* (JCQ)
- *A guide to the special consideration process* (JCQ)
- *Collaborative and consortium arrangements for the delivery of vocational qualifications policy* (Pearson)
- *UK information manual* (updated annually and available in hard copy) **or** *Entries and information manual* (available online) (Pearson)
- *Distance learning and assessment policy* (Pearson).

Publisher information

Any publisher can seek endorsement for their resources and, if they are successful, we will list their BTEC resources on our website.

13 Glossary

General terminology used in specification

Term	Description
Level	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 students; for example, lectures, tutorials, online instruction and supervised study. Units may vary in size.
Total Qualification Time (TQT)	This indicates the total number of hours that a typical student will take to complete the qualification. This is in terms of both guided learning hours and unguided learning; for example, private study, time spent in the workplace to master skills.
Learning outcomes	The learning outcomes of a unit set out what a student knows, understands or is able to do as the result of a process of learning.
Assessment criteria	The assessment criteria specify the standard a student 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, skills and understanding required for achievement of the unit. It enables centres to design and deliver a programme of learning that will enable students to achieve each learning outcome and to meet the standard determined by the assessment criteria.
Summative assessment	Assessment that takes place after the programme of learning has taken place.
Valid assessment	The assessment assesses the skills or knowledge/understanding in the most sensible, direct way to measure what it is intended to measure.
Reliable assessment	The assessment is consistent, and the agreed approach delivers the correct results on different days for the same students and different cohorts of students.

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

Pearson Education Limited. Registered in England and Wales No. 872828
Registered Office: 80 Strand, London WC2R 0RL.

VAT Reg No GB 278 537121

Pearson
BTEC

Publication code:
VQ000350