L3

Pearson Level 3 Alternative Academic Qualification
BTEC National in

Information Technology (Extended Certificate)

Specification

Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate)

Specification

First teaching September 2025

First certification from 2026

Issue 5

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.

This specification is Issue 5. Key changes are summarised on the next page. We will inform centres of any changes to this issue. The latest issue can be found on our website.

Welcome

BTEC Nationals are widely recognised by higher education and industry as the vocational qualification of choice at Level 3. They provide students with meaningful and practical learning experiences across a range of career sectors to prepare them to progress to higher education as a route to graduate-level employment.

Recent data has shown that one in five adults of working age in the UK has a BTEC qualification. What's more, well over 90,000 BTEC students apply to UK universities every year and their BTEC Nationals are accepted by over 150 UK universities and other higher education institutions for relevant degree programmes either on their own or in combination with A Levels.

Why are BTECs so successful?

BTECs embody a fundamentally student-centred approach to the curriculum, with a flexible, unit-based structure and knowledge applied through a balanced combination of assignments and examinations. They enable the holistic development of the practical, interpersonal and thinking skills required to succeed in higher education and employment.

When creating these BTEC Nationals we focused on the skills and personal attributes needed to navigate the future, and have worked with many higher education providers, professional bodies, colleges and schools to ensure that their needs are met. Employers are looking for future employees with a thorough grounding in the latest industry requirements and work-ready skills such as critical thinking and problem solving. Higher education needs students who have experience of research, extended writing and meeting deadlines.

We have addressed these requirements by:

- Facilitating and guiding the development of transferable skills through the design and delivery of the qualifications, using a holistic and practical framework which is based on recent research into the most critical skills needed to navigate the future. This Transferable Skills framework has been used to embed transferable skills in the qualifications where they naturally occur and also to signpost opportunities for delivery and development as a part of the wider BTEC learning experience.
  See page 6 for further information.

- Supporting the delivery of Sustainability Education and Digital Skills development naturally through the content design of the qualifications. Mapping is provided for each qualification to identify where the opportunities for teaching and learning exist.

- Updating sector-specific content to ensure it is relevant and future-facing.

- Implementing a consistent approach to assessment with a balanced combination of internal and external assessments to better engage students, make the qualifications more accessible for them and more manageable for centres to deliver.

We are providing a wealth of support, both resources and people, to ensure that students and their teachers have the best possible experience during their course. See Section 5 for details of the support we offer.

This specification document should be used in conjunction with the *Pearson Level 3 Alternative Academic Qualification BTEC National Specification Supplementary Information* document which is available on our website.

A word to students

Today's BTEC Nationals will require commitment and hard work, as you would expect of the most respected applied learning qualification in the UK. You will have to complete a range of units, be organised, take some assessments that we will set and mark and undertake practical tasks and assignments. But you can feel proud to achieve a BTEC because, whatever your plans in life – whether you decide to study further, go on to work or an apprenticeship – your BTEC National will be your passport to success in the next stage of your life.

Good luck, and we hope you enjoy your course.

Summary of changes to Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate) specification Issue 5

Summary of changes made between previous issue and this issue	Page number
Content A1.3.1 in Unit 1 has been updated from system diagrams to network diagrams	22

Earlier issue(s) show(s) previous changes.

If you need further information on these changes or what they mean, please contact us via our website at: qualifications.pearson.com/en/support/contact-us.html.

Contents

1 Introduction

Why choose Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate)?

We've listened to feedback from all parts of the Information Technology subject community, including higher education. We've used this opportunity of curriculum change to redesign qualifications so that they reflect the demands of a truly modern and evolving digital environment – qualifications that enable your students to apply themselves and give them the skills to succeed in their chosen pathway.

The Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate) allows students to study the fundamental knowledge of Information Technology covering the role and implications of using Information Technology systems and cyber-security threats and how to manage attacks. Students will also develop important skills for creating websites to meet a specific purpose and to manage data through the development of a relational database solution.

There are two examined units and two internally assessed units where students will engage in practical tasks to develop their Information Technology skills and knowledge.

The qualification is designed to be taken alongside A Levels as part of a study programme and can link to learning in A Level Mathematics and A Level Business Studies. It is intended for students that wish to progress into higher education as a pathway to employment.

Total Qualification Time

For all regulated qualifications, Pearson specifies a total number of hours that it is estimated students will require to complete and show achievement for the qualification: this is the Total Qualification Time (TQT). Within 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 teachers and assessors in teaching, supervising and invigilating students. Guided learning includes the time required for students to complete external assessment under examination or supervised conditions.

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

BTEC Nationals have been designed around the number of hours of guided learning expected. Each unit in the qualification has a GLH value of 60, 90 or 120. There is then a total GLH value for the qualification.

Each qualification has a TQT value. This may vary within sectors and across the suite depending on the nature of the units in each qualification and the expected time for other required learning.

The following table shows the qualifications in this sector and their GLH and TQT values.

Qualification title	Size and structure	Summary purpose
Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Certificate) (from 2026)	180 GLH (238 TQT) Equivalent in size to half an A Level. 2 units of which both are mandatory and 1 is external. Mandatory content (100%). External assessment (66%).	The Certificate is for students who are interested in learning about Information Technology and how it applies in multiple sectors alongside other fields of study, with a view to progressing to a wide range of higher education courses, not necessarily in the IT sector. It is designed to be taken as part of a programme of study that includes A Levels.
Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate)	360 GLH (468 TQT) Equivalent in size to one A Level. 4 units of which 4 are mandatory and 2 are external. Mandatory content (100%). External assessment (66.6%).	The Extended Certificate is for students who are interested in learning about the Information Technology sector alongside other fields of study, with a view to progressing to a wide range of higher education courses, not necessarily in Information Technology-related subjects. It is designed to be taken as part of a programme of study that includes A Levels.

Structures of the qualifications at a glance

This table shows all the units and the qualifications to which they contribute. The full structure for this Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate) is shown in *Section 3 Structure*. **You must refer to the full structure to select units and plan your programme.**

Key
Externally assessed units are shown in bold
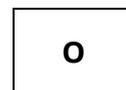
| | M | Mandatory units | | O | Optional units |

Unit (number and title)	Unit size (GLH)	Certificate (180 GLH)	Extended Certificate (360 GLH)
1 Information Technology Systems	**120**	**M**	**M**
2 Cyber security and Incident Management	**120**		**M**
3 Website Development	**60**	M	M
4 Relational Database Development	**60**		M

Qualification and unit content

Pearson has developed the content of the new BTEC Nationals in collaboration with representatives from higher education and relevant professional bodies. In this way, we have ensured that content is up to date and that it includes the knowledge, understanding, skills and attributes required in the sector.

Centres should ensure that delivery of content is kept up to date. Some of the units within the specification may contain references to legislation, policies, regulations and organisations, which may not be applicable in the country you deliver this qualification in (if teaching outside of England), or which may have gone out-of-date during the lifespan of the specification. In these instances, it is possible to substitute such references with ones that are current and applicable in the country you deliver subject to confirmation by your Standards Verifier.

Assessment

Assessment is specifically designed to fit the purpose and objective of the qualification. It includes a range of assessment types and styles suited to vocational qualifications in the sector. There are three main forms of assessment that you need to be aware of: external, internal and synoptic.

Externally assessed units

Each external assessment for a BTEC National is linked to a specific unit. All of the units developed for external assessment are of 60, 90 or 120 GLH to allow students to demonstrate breadth and depth of achievement. Each assessment is taken under specified conditions, then marked by Pearson and a grade awarded. Students are permitted to resit the examination twice. This equates to three attempts in total: one inclusive of registration, the remaining two attempts as resits. If students resit an examined unit, the best grade achieved will count towards their overall qualification grade, not necessarily the most recent sitting. External assessments are available twice a year. For detailed information on the external assessments, please see the table in *Section 3.* For further information on preparing for external assessment, see the *Pearson Level 3 Alternative Academic Qualification BTEC National Specification Supplementary Information* document which is available on our website.

Internally assessed units

Internally assessed units are assessed by a Pearson Set Assignment Brief (PSAB), which is set by Pearson, marked by you and subject to external standards verification. Before you assess you will need to become an approved centre, if you are not one already. You will need to prepare to assess using the guidance in the *Pearson Level 3 Alternative Academic Qualification BTEC National Specification Supplementary Information* document, which is available on our website.You will make grading decisions based on the requirements and supporting guidance given in the units. Where a student has not

achieved their expected level of performance for an assignment, they may be eligible for one resubmission of improved evidence for each assignment submitted if authorised by the Lead Internal Verifier.

To ensure any resubmissions are fairly and consistently implemented for all students, the Lead Internal Verifier can only authorise a resubmission if certain conditions are met. If the Lead Internal Verifier does authorise a resubmission, it must be completed within 15 working days of the student receiving the results of the assessment.

Feedback to students can only be given to clarify areas where they have not achieved expected levels of performance. Students cannot receive any specific guidance or instruction about how to improve work to meet assessment criteria or be given solutions to questions or problems in the tasks.

If a student has still not achieved the targeted pass criteria following the resubmission of improved evidence for an assignment, the Lead Internal Verifier may authorise, under exceptional circumstances, one retake opportunity to meet the required pass criteria. The retake can be of a task or subset of the Pearson Set Assignment Brief that is of evidence in a new or revised form. The deadline for submission of the retake must fall within the same academic year.

Synoptic assessment

Synoptic assessment requires students to demonstrate that they can identify and use effectively, in an integrated way, an appropriate selection of skills, techniques, concepts, theories and knowledge from across the whole sector as relevant to a key task. Synoptic links between units are flagged within the units. Please refer to *Unit 1: Information Technology Systems* and *Unit 3: Website Development* for further details.

Language of assessment

Assessment of the internal and external units for these qualifications will be available in English. All student work must be in English. A student taking the qualifications may be assessed in British or Irish Sign Language where it is permitted for the purpose of reasonable adjustment.

For information on reasonable adjustments see the *Pearson Level 3 Alternative Academic Qualification BTEC National Specification Supplementary Information* document, which is available on our website.

Grading for units and qualifications

Achievement in the qualification requires a demonstration of depth of study in each unit, assured acquisition of a range of practical skills required for progression to higher education, and successful development of transferable skills. Students achieving a qualification will have completed all units.

Units are assessed using a grading scale of Distinction (D), Merit (M), Pass (P), Near Pass (N) and Unclassified (U). The grade of Near Pass is used for externally assessed units only. All mandatory and optional units contribute proportionately to the overall qualification grade, for example a unit of 120 GLH will contribute double that of a 60 GLH unit.

BTEC National qualifications are graded using a scale of P to D*, **or** PP to D*D*, **or** PPP to D*D*D* depending on the size of the qualification. Please see *Section 6* for more details. The relationship between qualification grading scales and unit grades will be subject to regular review as part of Pearson's standards monitoring processes on the basis of student performance and in consultation with key users of the qualification.

UCAS tariff points

The BTEC Nationals attract UCAS points. Please go to the UCAS website for full details of the points allocated.

Preparing students for the future

Transferable skills

Recent future skills reports have highlighted the growing importance of transferable skills for students to succeed in their careers and lives in this fast-changing world.

Following research and consultation with FE educators and higher education institutions, Pearson has developed a Transferable Skills Framework to facilitate and guide the development of transferable skills through this qualification. The Framework has four broad skill areas, each with a cluster of skills as shown below:

1. **Managing Yourself**: (1) Taking personal responsibility; (2) Personal strengths and resilience; (3) Career orientation planning; (4) Personal goal setting

2. **Effective Learning**: (1) Managing own learning; (2) Continuous learning; (3) Secondary research skills (4) Primary research skills

3. **Interpersonal Skills**: (1) Written communications; (2) Verbal and non-verbal communications; (3) Teamwork; (4) Cultural and social intelligence

4. **Solving Problems**: (1) Critical thinking (2) Problem solving; (3) Creativity and innovation

Each transferable skill has a set of descriptors that outline what achievement of the skill looks like in practice. Each unit in the qualification will show whether a transferable skill has been:

1. fully embedded through the design of the teaching and learning content and assessment of the unit. Skills that are embedded are 'naturally occurring' in that they are inherent to the unit content and don't require extension activities to deliver.

2. signposted as an opportunity for delivery and development and would require extension activities to deliver.

Units will show a summary of the transferable skills that have been embedded or signposted and *Appendix 2* shows the descriptors for each skill across all the skill clusters.

More information on the framework, its design and relevance for student progression is available in the *BTEC Transferable Skills Guide for Teachers*. Resources and guidance to support teachers in the delivery and development of these skills will be available in the Planning and Teaching Guide for this qualification and through our training offer.

Digital skills

Digital skills are required in every industry as well as in everyday life and, with the acceleration of automation and AI in industry it is critical for students to understand how digital technologies are relevant and applied in the context of the sector they are studying.

With this in mind, we have used the Digital Skills Framework published by IFATE as a frame of reference to identify opportunities for the delivery and development of digital skills in this qualification.

This Digital Skills framework has five categories with specific digital characteristics that apply in varying extent across sectors:

- **Problem Solving** – The use of digital tools to analyse and solve problems
- **Digital Collaboration and Communication** – Using digital tools to communicate and share information with stakeholders
- **Transacting Digitally** – Using digital tools to set up accounts and pay for goods/services
- **Digital Security** – Identify threats and keep digital tools safe
- **Handling Data Safely and Securely** – Follow correct procedures when handling personal and organisational data

Opportunities to develop these digital skills are identified where they are relevant and appropriate to a sector, meaning that:

- Where they naturally occur
- Where embedding adds no assessment burden
- Where embedding will enhance a student's skills and knowledge in the sector.

Appendix 3 shows a mapping of the teaching and learning content to the five categories of the framework to show where opportunities to develop these digital skills exist in this qualification.

Sustainability skills

To help students develop sustainability skills, practices and mindset, we have designed content in this qualification aligned to the [UNESCO Sustainable Development Goals](#) (17 SDGs), that are relevant and appropriate to the sector. The SDGs are the most common point of reference for content that addresses sustainability and provides a useful and pragmatic way of organising this content.

Sustainability knowledge and understanding may be included in the teaching and learning content but not directly assessed. Additionally, it could be assessed – the approach chosen for each unit is based on the relevance of the sustainability skills, knowledge and understanding to the purpose and scope of the unit.

Appendix 4 shows a mapping of the teaching and learning content to the relevant SDGs to show where sustainability concepts have been included in this qualification.

2 Qualification purpose

Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate)

In this section you will find information on the purpose of this qualification and how its design meets that purpose through the qualification objective and structure. We publish a full 'Statement of Purpose' for each qualification on our website. These statements are designed to guide you and potential students to make the most appropriate choice of qualification at recruitment.

Who is this qualification for?

The Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate) is an Alternative Academic Qualification (AAQ) designed for post-16 students with an interest in the Digital sector and aiming to progress to higher education as a route to graduate level employment.

Equivalent to one A Level in size, it is suitable for students looking to develop their applied knowledge and skills in Information Technology as part of a study programme alongside A Levels.

What will the student study as part of this qualification?

The qualification has been developed in consultation with higher education representatives and sector experts to ensure students have the knowledge, understanding and skills they need to progress to, and thrive, in higher education.

The qualification has four mandatory units covering the following topics:

- **Information Technology Systems** – Information technology systems, including the relationship between software and hardware, and the issues related to IT systems
- **Cyber Security and Incident Management** – Types of cyber security attacks, the vulnerabilities in networked systems and how to plan and respond to attacks
- **Website Development** – The development tools, techniques and processes used in website development and how to test usability, functionality and fitness for purpose
- **Relational Database Development** – Structure of data, data design and database management systems (DBMS).

What knowledge and skills will the student develop as part of this qualification and how might these be of use and value in further studies?

Students will develop the following knowledge and skills:

- Knowledge of digital technologies and how organisations plan digital projects and follow a project lifecycle
- Understanding of organisation structures and processes and how to embed digital safety to keep data and assets secure
- Technical skills to:
  o design and build a website to meet user requirements using relevant tools and techniques, including testing for usability, functionality and fitness for purpose
  o follow a design methodology to create and develop a database design to meet user requirements, including testing the solution
- Transferable skills such as creativity and innovation, written communications, critical thinking and taking personal responsibility.

Students will develop the ability to apply digital concepts to different sectors which is beneficial to the analytical approach included in many degrees. The ability to take personal responsibility and written communication skills will develop students' ability to manage their own work and independently create extended writing tasks which is a good foundation for academic success.

Which subjects will complement this qualification?

The following subjects would be suitable to combine with this qualification:

- Business
- Mathematics
- Psychology
- Art & Design

What further learning will this qualification lead to?

This qualification can lead to progression to the following degrees:

- BA Business Studies
- BSc Information Systems
- BSc Computer Science

3 Structure

Qualification structure

Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate)

Students must complete 4 mandatory units.

See *Section 6* for rules on qualification awarding.

Mandatory units – students complete all units

Unit number	Unit title	GLH	Type	How assessed
1	Information Technology Systems	120	**Mandatory**	External
2	Cyber Security and Incident Management	120	**Mandatory**	External
3	Website Development	60	**Mandatory**	Internal
4	Relational Database Development	60	**Mandatory**	Internal

External assessment

66.6% of the total qualification GLH is made up of external assessment. A summary is given below. See the unit content and sample assessment materials for more information.

Unit	Type	Availability
Unit 1: Information Technology Systems	• An external examination set and marked by Pearson • 90 marks	**January and May/June** **First assessment May/June 2026**
Unit 2: Cyber Security and Incident Management	• An external examination set and marked by Pearson • 90 marks	**January and May/June** **First assessment May/June 2026**

Synoptic assessment

The assessment of synoptic knowledge requires students to apply learning from one unit to the assessment in another unit. Within the assessment for *Unit 3: Website Development*, students will be assessed on underpinning knowledge, ideas and concepts from *Unit 1: Information Technology Systems*. Synoptic links are flagged within the units.

There might be some further naturally occurring synoptic opportunities across the qualification where students can synthesise their learning. These will be outlined in the Planning and Teaching Guide to help with planning for your teaching.

4 Units

Understanding your units

The units in this specification set out our expectations of assessment in a way that helps you to prepare your students for assessment. The units help you to undertake assessment and quality assurance effectively.

Each unit in the specification is set out in a similar way. There are two types of unit format:

- Internally assessed units
- Externally assessed units.

This section explains how the units work. It is important that all teachers, assessors, internal verifiers and other staff responsible for the programme review this section.

Internally assessed units

Section	Explanation
Unit number	The number is in a sequence in the sector. Numbers may not be sequential for an individual qualification.
Unit title	This is the formal title that we always use and it appears on certificates.
Unit level	All units are Level 3 on the national framework.
Unit type	This confirms that the unit is internally assessed. See structure information in *Section 3* for full details.
GLH	Units may have a Guided Learning Hours (GLH) value of 120, 90 or 60. This indicates the numbers of hours of teaching, directed activity and assessment expected. It also shows the weighting of the unit in the final qualification grade.
Unit in brief	A brief formal statement on the content of the unit that is helpful in understanding its role in the qualification. You can use this in summary documents, brochures etc.
Unit introduction	This is designed with students in mind. It indicates why the unit is important, how learning is structured and how learning might be applied when progressing to employment or higher education.
Learning aims	These help to define the scope, style and depth of learning of the unit. You can see where students should be learning standard requirements ('understand') or where they should be actively researching ('investigate'). You can find out more about the verbs we use in learning aims in *Appendix 1*.

Section	Explanation
Summary of unit	This helps teachers to see the main content areas against the learning aims and the structure of the assessment at a glance.
Content	This sets out the required teaching content of the unit. Content is compulsory except where shown as 'e.g.'. Students should be asked to complete summative assessment only after the teaching content for the unit or learning aim(s) has been covered.
Assessment criteria	Each learning aim has Pass and Merit criteria. Each assignment has at least one Distinction criterion. A full glossary of terms used is given in *Appendix 1*.

Distinction criteria represent outstanding performance in the unit. Some criteria require students to draw together learning from across the learning aims. |
Transferable skills	This summarises the transferable skills present within this unit. The key helps to identify whether they are signposted but require additional assessment, embedded and achieved on completion or not present in this unit.
Essential information for Pearson Set Assignment Brief (PSAB)	This shows a brief summary of the activities required for the mandatory Pearson Set Assignment Brief. Centres must download and use the mandatory PSAB without alteration or contextualisation.
Further information for teachers and assessors	This gives you information to support the implementation of assessment. It is important that this is used carefully alongside the assessment criteria and PSAB.
Resource requirements	Any specific resource requirements that you need to be able to teach and assess are listed in this section.
Essential information for assessment decisions	This information gives guidance for each learning aim or assignment of the expectations for Pass, Merit and Distinction standard. This section contains examples and essential clarification.
Links to other units	This shows you the main relationship between units. This can help you to structure your programme and make best use of materials and resources.

Externally assessed units

Section	Explanation
Unit number	The number is in a sequence in the sector. Numbers may not be sequential for an individual qualification.
Unit title	This is the formal title that we always use and it appears on certificates.
Unit level	All units are Level 3 on the national framework.
Unit type	This confirms that the unit is externally assessed. See structure information in *Section 3* for full details.
GLH	Units may have a Guided Learning Hours (GLH) value of 120, 90 or 60. This indicates the numbers of hours of teaching, directed activity and assessment expected. It also shows the weighting of the unit in the final qualification grade.
Unit in brief	A brief formal statement on the content of the unit that is helpful in understanding its role in the qualification. You can use this in summary documents, brochures etc.
Unit introduction	This is designed with students in mind. It indicates why the unit is important, how learning is structured and how learning might be applied when progressing to employment or higher education.
Summary of assessment	This sets out the type of external assessment used and the way in which it is used to assess achievement.
Assessment outcomes	These show the hierarchy of knowledge, understanding, skills and behaviours that are assessed. Includes information on how this hierarchy relates to command terms in sample assessment materials (SAMs).
Content	For external units all content is obligatory. The depth of content is indicated in the assessment outcomes and sample assessment materials (SAMs). The content will be sampled through the external assessment over time, using the variety of questions shown.
Transferable skills	This summarises the transferable skills present within this unit. The key helps to identify whether they are signposted but require additional assessment, embedded and achieved on completion or not present in this unit.
Key terms typically used in assessment	These definitions will help you analyse requirements and prepare students for assessment.
Resources	Any specific resource requirements that you need to be able to teach and assess are listed in this section.

Index of units

Unit 1: Information Technology Systems

Level: 3

Unit type: External

Guided learning hours: 120

Unit in brief

Students will study the role of Information Technology (IT) systems and the implications of their use in personal and professional situations. Students will gain knowledge and understanding of issues relating to the use of IT in personal and professional situations.

Unit introduction

IT systems have a significant role in the world around us and play a part in almost everything we do. Having sound knowledge and understanding of how to effectively select and use appropriate IT systems will benefit you personally and professionally.

You will explore the relationships between the hardware and software that form an IT system, how systems work individually and together, and the relationship between the user and the system. You will examine issues related to the use of IT systems and the impact that they have on organisations and individuals.

This unit will give you a fundamental understanding of all areas of IT, supporting your progression to an IT-related higher education course.

Summary of assessment

The unit will be assessed through one examination of 90 marks lasting 2 hours.

Students will be assessed through a number of short- and long-answer questions. The questions will assess knowledge and understanding of IT systems and the implications of their use in personal and professional situations.

The assessment availability is twice a year in January and May/June. The first assessment availability is May/June 2026.

Sample assessment materials will be available to help centres prepare students for assessment.

Assessment outcomes

AO1 Demonstrate knowledge and understanding of information technology systems, terminology, concepts and processes.

AO2 Apply knowledge and understanding of information technology systems, terminology, concepts and processes.

AO3 Analyse and evaluate the factors and implications of information technology systems.

[SP-CT]

Content

The essential content is set out under content areas. Students must cover all specified content before the assessment.

A: Explore the concepts and implications of the use of, and relationships among devices that form IT systems

A1 Functions and use of digital devices, and the notation used to represent the design of IT systems

Students should apply their knowledge and understanding of the features and uses of digital devices in IT systems to meet the needs of individuals and organisations. Students should apply their knowledge of notation used in designing IT systems and flowcharts. This knowledge is essential for the effective use of technology in both personal and professional settings.

A1.1 Features of digital devices that form part or all of IT systems:

    A1.1.1 personal computers

    A1.1.2 multifunctional devices

    A1.1.3 mobile devices

    A1.1.4 servers

- file
- application
- web

    A1.1.5 entertainment systems

    A1.1.6 digital cameras

- still
- video

    A1.1.7 navigation systems

    A1.1.8 communication devices and systems

    A1.1.9 embedded systems

- Sensors
- Internet of Things (IoT).

A1.2 Function and use of the above digital devices for:

    A1.2.1 personal

    A1.2.2 education and training

    A1.2.3 social

    A1.2.4 retail

    A1.2.5 manufacturing

A1.2.6   healthcare

A1.2.7   creative tasks

A1.2.8   automation and robotics.

A1.3   Forms of notation used to design IT systems:

A1.3.1   network diagrams

A1.3.2   flowcharts.

A2 Peripheral devices and media

Students should apply their knowledge and understanding of the features and uses of peripheral devices and media in IT systems to meet the needs of individuals and organisations.

A2.1   Features and uses of peripheral devices used with other digital devices to form part of an IT system:

A2.1.1   input devices

A2.1.2   output devices

A2.1.3   storage devices.

A2.2   Assistive technologies

A2.2.1   adaptive keyboards

A2.2.2   screen readers

A2.2.3   braille displays

A2.2.4   screen magnifiers

A2.2.5   head pointers

A2.2.6   single switch entry devices

A2.2.7   foot switches

A2.2.8   sip-and-puff switches

A2.2.9   eye-tracking software

A2.2.10 text-to-speech software.

A2.3   Characteristics and implications of storage media used to form part of an IT system.

A2.3.1   capacity

A2.3.2   cost

A2.3.3   speed

A2.3.4   compatibility

A2.4   Data processing.

A2.4.1   manual

A2.4.2   automatic

A3 Computer software in an IT system

Students should know and understand the concepts, implications and impact on individuals and organisations of the use of, and relationships between hardware and software.

A3.1   Types of operating systems:

    A3.1.1   batch

    A3.1.2   distributed

    A3.1.3   multitasking

    A3.1.4   network OS

    A3.1.5   real-time OS

    A3.1.6   mobile OS

    A3.1.7   single use

    A3.1.8   multi-user

A3.2   Role of the operating system in managing:

    A3.2.1   networking (protocols, connections, data transmission and reception, resource allocation and monitoring)

    A3.2.2   security (access control, malware protection, encryption, firewall)

    A3.2.3   memory management (allocation and deallocation, memory protection, virtual memory, swapping and paging)

    A3.2.4   multi-tasking (process scheduling, CPU time management, context switching)

    A3.2.5   device drivers (installation and loading, communication, driver management and updates, error handling, resource allocation)

    A3.2.6   user accounts (user authentication, user profiles, account management tools).

A3.3   Types, uses and features of software:

    A3.3.1   utility

    A3.3.2   application.

A3.4   Factors impacting the choice and use of operating system and application software.

    A3.4.1   cost

    A3.4.2   security

    A3.4.3   hardware and software compatibility

    A3.4.4   features

    A3.4.5   business and/or user needs

    A3.4.6   performance.

A3.5 Types of user interface and factors affecting the choice of user interface:

A3.5.1 command line

A3.5.2 menu-driven

A3.5.3 graphical user

A3.5.4 touchscreen graphical user.

A3.6 Principles and implications of open source and proprietary software:

A3.6.1 operating systems

A3.6.2 application software.

A3.7 Features of common file types and formats used for:

A3.7.1 images

A3.7.2 audio

A3.7.3 videos

A3.7.4 application software.

A4 Choosing IT systems

Students should know and understand how the features of an IT system can affect its performance and the factors impacting on the choice.

A4.1 Factors affecting the choice of IT systems:

A4.1.1 user needs

A4.1.2 specifications

A4.1.3 compatibility

A4.1.4 connectivity

A4.1.5 cost

A4.1.6 efficiency

A4.1.7 implementation

- timescales
- testing
- migration to new system(s)
- downtime

A4.1.8 productivity

A4.1.9 security.

A4.2 Features and implications of IT systems used by organisations for:

A4.2.1 stock control

A4.2.2 data logging

A4.2.3 data analysis

A4.2.4 general office tasks

A4.2.5 creative tasks

A4.2.6 advertising

A4.2.7 manufacturing

A4.2.8 security

A4.2.9 automation.

A4.3 Impact and implications for organisations of IT systems in terms of:

A4.3.1 user experience

- ease of use

- performance

- availability

- accessibility

A4.3.2 employee and customer needs

A4.3.3 cost

A4.3.4 implementation

- timescales

- testing

- migration to new system(s)

- downtime

A4.3.5 replacement or integration with current systems

A4.3.6 productivity

A4.3.7 working practices

A4.3.8 staff training needs

- Initial

- ongoing

A4.3.9 user support

A4.3.10 security.

A5 Emerging technologies

Students should understand how emerging technologies can be used by individuals and organisations.

A5.1 The concepts and implications of how emerging technologies and artificial intelligence (AI) affect the performance of IT systems.

A5.2 Implications of emerging technologies and AI on the personal use of IT systems.

A5.3 Implications of emerging technologies and AI on the use of IT systems in organisations.

B: Transmitting data

The essential content topics require understanding of the concepts, processes and implications of transmitting data within and between IT systems.

B1 Connectivity

B1.1 Wireless and wired methods of connecting devices and transmitting data within and between IT systems.

> **B1.1.1** Bluetooth
>
> **B1.1.2** USB
>
> **B1.1.3** Wi-Fi
>
> **B1.1.4** Ethernet

B1.2 How the features of connection types can meet the needs of individuals and organisations.

B1.3 Implications of selecting and using different connection types.

B1.4 Impact of connection types on the performance of an IT system.

B2 Networks

Students should know the concepts and implications for individuals and organisations of connecting devices to and from a network.

B2.1 Network topologies:

> **B2.1.1** star
>
> **B2.1.2** ring
>
> **B2.1.3** bus.

B2.2 Types of networks:

> **B2.2.1** Personal Area Network (PAN)
>
> **B2.2.2** Local Area Network (LAN)
>
> **B2.2.3** Wide Area Network (WAN)
>
> **B2.2.4** Virtual Private Network (VPN).

B2.3 Factors affecting the choice of network:

> **B2.3.1** user needs
>
> **B2.3.2** specifications
>
> **B2.3.3** connectivity
>
> **B2.3.4** cost
>
> **B2.3.5** efficiency
>
> **B2.3.6** compatibility

B2.3.7 implementation

- timescales

- testing

- downtime

B2.3.8 productivity

B2.3.9 security.

B2.4 How the features of a network and its component parts affect the performance of an IT system.

B3 Issues relating to transmission of data

Students should know and understand how the features and processes of data transmission affect the use and performance of IT systems.

B3.1 Protocols used to govern and control data transmission for common tasks:

B3.1.1 email

- SMTP

- POP

- IMAP

B3.1.2 voice and video call over the internet

B3.1.3 web pages

- HTTP

- HTTPS

B3.1.4 secure payment systems

B3.2 Security issues and considerations when transmitting data over different connection types and networks.

B3.3 Factors affecting and implications of bandwidth and latency.

B3.4 Implications of common file types and formats used for:

B3.4.1 images

B3.4.2 audio

B3.4.3 videos

B3.4.4 application software

B3.5 Factors affecting the choice of compression types:

B3.5.1 lossy

B3.5.2 lossless.

B3.6 Use and implications of codecs when using and transmitting audio and video in digital format.

C: Operating online

The essential content topics require understanding of the implications for individuals and organisations of using online IT systems.

C1 Online systems

Students should know and understand the features, impact and implications of the use of online IT systems to store data and perform tasks.

C1.1 Cloud computing models

    C1.1.1 private cloud

    C1.1.2 public cloud

    C1.1.3 hybrid cloud

    C1.1.4 Infrastructure as a Service (IaaS)

    C1.1.5 Software as a Service (SaaS)

    C1.1.6 Platform as a Service (PaaS)

C1.2 Impact and implications of using cloud computing for individuals and organisations.

C1.3 Systems that enable and support remote working:

    C1.3.1 VPNs

    C1.3.2 remote desktop technologies.

C1.4 The way factors affect the use and selection of online systems:

    C1.4.1 security

    C1.4.2 cost

    C1.4.3 ease of use

    C1.4.4 features

    C1.4.5 connectivity

    C1.4.6 scalability.

C2 Online communities

Students should know and understand the features of online communities and the implications of their widespread use for individuals and organisations.

C2.1 Ways of communicating and interacting with online communities:

    C2.1.1 social media

    C2.1.2 blog/vlog

    C2.1.3 wiki

    C2.1.4 chatrooms

    C2.1.5 instant messaging

    C2.1.6 podcasts

    C2.1.7 forums.

C2.2 Considerations for individuals and organisations of using and accessing online communities:

C2.2.1 user experience

- ease of use
- performance
- availability
- accessibility

C2.2.2 meeting user needs

C2.2.3 cost

C2.2.4 privacy

C2.2.5 security

C2.2.6 downtime

C2.2.7 training

C2.2.8 integration with current systems

C2.2.9 productivity

C2.2.10 working practices and company policies.

D: Protecting data and information

The essential content topics require understanding of the issues and implications of storing and transmitting information in digital form.

D1 Threats to data, information, and systems

Students should know and understand the types of accidental and malicious threats to the security and integration of data, held in and used by IT systems.

D1.1 Types of external threats to data:

D1.1.1 viruses and other malware

D1.1.2 unauthorised access – hackers

D1.1.3 accidental damage

D1.1.4 social engineering.

D1.1.5 natural disasters

D1.2 Types of internal threats to data:

D1.2.1 access to inappropriate websites

D1.2.2 accidental disclosure of data

D1.2.3 stealing/leaking information

D1.2.4 use of portable devices.

D1.3 Impact on individuals and organisations from threats to data, information and systems:

 D1.3.1 loss of data

 D1.3.2 financial loss due to legal action

 D1.3.3 loss of customers due to public image.

D2 Protecting data

Students should know the uses and implications of systems and procedures used to protect the data of individuals and organisations.

D2.1 Techniques used to protect data and systems:

 D2.1.1 file permissions

 D2.1.2 access levels

 D2.1.3 backup and recovery procedures

 D2.1.4 passwords/multi-factor authentication

 D2.1.5 biometrics

 D2.1.6 physical access control

 D2.1.7 digital certificates.

D2.2 Features and functions of using antivirus software to protect data.

D2.3 Features and functions of using firewalls to protect data.

D2.4 Features and functions of encryption methods to protect:

 D2.4.1 stored data

 D2.4.2 data during transmission

 D2.4.3 data in secure websites (HTTPS).

E: Impact of using IT systems

The essential content topics require understanding of the uses, issues and implications of IT systems and their impact on individuals and organisations.

E1 Online services

Understand how the features of online services are used to meet the needs of individuals and organisations.

E1.1 Features and implications of using online services to support:

 E1.1.1 retail

 E1.1.2 financial services

 E1.1.3 education and training

 E1.1.4 news and information

E1.1.5 entertainment and leisure

E1.1.6 booking systems.

E1.2 Uses, impact and implications for individuals and organisations of:

E1.2.1 transactional data

E1.2.2 targeted marketing

E1.2.3 collaborative working

E1.2.4 remote working.

E2 Using and manipulating data

Understand the uses, processes and implications for individuals and organisations of accessing and using data and information in digital form.

E2.1 Sources of data:

E2.1.1 primary

E2.1.2 secondary.

E2.2 Methods of ensuring reliability of information.

E2.3 Methods of collecting data and opinions:

E2.3.1 survey

E2.3.2 questionnaire

E2.3.3 focus groups

E2.3.4 interview.

E2.4 Reasons for ensuring data accuracy.

E2.5 Methods of ensuring data accuracy:

E2.5.1 verification

E2.5.2 validation.

E2.6 Characteristics and considerations of user interfaces for data collection and processing systems:

E2.6.1 ease of use

E2.6.2 accessibility

E2.6.3 error reduction

E2.6.4 functionality

E2.6.5 performance

E2.6.6 compatibility.

F: Issues

The essential content topics require understanding of the concepts, impacts, and implications of moral, ethical and legal issues relating to the use of IT systems.

F1 Moral and ethical issues

Understand the moral and ethical factors and implications of using information technology for individuals and organisations.

F1.1   Moral and ethical factors and implications of the use of information technology:

F1.1.1   privacy

F1.1.2   environmental impact

F1.1.3   unequal access to information technology

F1.1.4   access to assistive technology

F1.1.5   online behaviour and netiquette

F1.1.6   acceptable use policies.

F2 Legal issues

Understand the legal issues relating to the use of IT systems, and the implications for individuals and organisations.

F2.1   Role and impact of current legislation in protecting IT systems, users and their data from attack and misuse:

F2.1.1   computer misuse legislation

F2.1.2   copyright, designs and patents legislation

F2.1.3   copyright regulations (computer programs)

F2.1.4   health and safety and display screen equipment regulations

F2.1.5   data protection legislation

Transferable skills

Managing Yourself	Effective Learning	Interpersonal Skills	Solving Problems
MY – TPR	EL – MOL	IS – WC	SP – CT *
MY – PS&R	EL – CL	IS – V&NC	SP – PS
MY – COP	EL – SRS	IS – T	SP – C&I
MY – PGS	EL-PRS	IS – C&SI	

Table key

*	Signposted to indicate opportunities for development as part of wider teaching and learning.
√	Embedded in teaching, learning and assessment
blank	TS not embedded or signposted in unit

Key terms typically used in assessment

The following table shows the key terms that will be used consistently by Pearson in our assessments to ensure students are rewarded for demonstrating the necessary skills.

Please note: the list below will not necessarily be used in every paper/session and is provided for guidance only.

Command or term	Definition
Describe	Students provide an account of something or highlight several key features of a given topic. May also be used in relation to the stages of a process.
Discuss	Students consider the different aspects in detail of an issue, situation, problem or argument and how they interrelate.
Draw	Students represent understanding using a diagram or flowchart.
Explain	Students identify a point and give a linked justification/exemplification of that point. The answer must contain some linked reasoning.
Evaluate	Students consider various aspects of a subject's qualities in relation to its context such as: strengths or weaknesses, advantages or disadvantages. They come to a judgement supported by evidence which will often be in the form of a conclusion.
Identify	Students select some key information from a given stimulus/resource.
State, name, give	Students recall one or more pieces of information

Unit 2: Cyber Security and Incident Management

Level: 3

Unit type: External

Guided learning hours: 120

Unit in brief

Students will study cyber security threats and vulnerabilities, the methods used to protect organisations against threats and managing security incidents.

Unit introduction

Our increasing reliance on computer systems and the data they contain makes us vulnerable to attacks from cyber criminals and to the loss of these systems if there is an accident or a natural disaster. As Information Technology (IT) system security is improved, more sophisticated methods of attack are developed, and it is important that organisations have robust plans in place to deal with a cyber security incident before it occurs. All IT professionals require a good understanding of the current threats to systems, how to apply appropriate and effective protection methods and how to manage a cyber security incident.

In this unit, you will examine the many types of cyber security attacks, the vulnerabilities in networked systems and the techniques that can be used to defend an organisation's networked systems. You will examine scenarios and explain appropriate protection measures for networked systems. You will also look at the forensic methods used to investigate cyber security incidents and analyse the suitability of those methods for a given scenario.

As IT systems evolve, there is an increasing need for IT professionals to protect networked systems and the information they contain, while providing enhanced features and benefits for organisations, customers and individuals. This unit will help prepare you for IT courses in higher education.

Summary of assessment

The unit will be assessed through one examination of 90 marks lasting 2 hours 15 minutes.

Students will be assessed through a number of short- and long-answer questions. Students will need to explore and relate to contexts and data presented. The questions will assess understanding of cyber security threats, the methods used to counter them and the forensics used to investigate an attack.

The assessment availability is twice a year in January and May/June. The first assessment availability is May/June 2026.

Sample assessment materials will be available to help centres prepare students for assessment.

Assessment outcomes

AO1 Demonstrate knowledge and understanding of cyber security terms, security threats, system vulnerabilities and security protection methods, forensic procedures and implications resulting from threats.

AO2 Apply knowledge and understanding to security threats, system vulnerabilities and security protection methods, forensic procedures and implications by selecting appropriate security tools and methods.

AO3 Analyse and evaluate security threats, system vulnerabilities and security protection methods, forensic procedures and implications for cyber security scenarios.

[SP-CT]

Content

The essential content is set out under content areas. Students must cover all specified content before the assessment. All topics require students to apply knowledge, analyse and evaluate.

A: Cyber security threats, system vulnerabilities and security protection methods

A1 Cyber security threats

Students should apply their knowledge and understanding of the function and impact of internal and external threats.

A1.1 Internal threats:

   A1.1.1 employee sabotage, deliberate and accidental

   - theft or loss of
      - physical equipment
      - data
      - software/licences
   - use of unauthorised software
      - license and legal liability issues
      - compatibility issues
      - interference with running of the network/other software
      - used for spying. harassment, illegal activities
      - used to avoid/interfere with monitoring, auditing, user/device supervision

   A1.1.2 accidental or deliberate damage

   - fire
   - flood
   - power loss
   - terrorism
   - other disasters

   A1.1.3 weak cyber security measures and unsafe practices

   - security of computer equipment and storage devices
   - security vetting of visitors
   - visiting untrustworthy websites

A1.1.4 accidental loss or disclosure of data/credentials

- human factors
  - negligence
  - poor training
  - not following security procedures
- inadequate monitoring and reporting
- weak security culture

A1.2 Function of external threats:

A1.2.1 malicious software (malware)

- viruses
  - boot sector
  - web script
  - macro
  - worm
  - rootkit
  - trojan
  - browser hijack
  - polymorphic
- spyware
  - keylogger/data thief
  - system monitor
  - mobile device tracker/stalkerware
  - web beacons and tracking cookies
- adware
  - potentially unwanted program (PUP)
  - legitimate adware
  - abusive or deceptive adware, legal and illegal
- ransomware
  - encryptors
  - lockers
  - scareware
  - leakware/doxware
- bots

A1.2.2 hacking – commercial, government, individuals

- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- browser hijack
- cyberwarfare
- data theft
- data tampering
  - back end – databases and other data stores
  - front end – web pages and other public facing displays

A1.2.3 sabotage – commercial, government, individuals, terrorism

- data poisoning
- data tampering
- data destruction
- fakes
  - images, video, audio, documents
  - using manual/traditional software methods
  - using Artificial Intelligence (AI)
- damage to/hijacking of
  - machinery
  - vehicles
  - internet connected devices
  - industrial processes
  - critical infrastructure – commercial and national

A1.2.4 social-engineering techniques used to obtain secure information by deception.

- phishing, vishing, smishing
- whaling, spear phishing
- Domain Name System (DNS) spoofing
- pretexting/impersonation

A1.2.5 physical security

- unauthorised access to secure areas
  - tailgating
  - forced entry
  - impersonation
  - coercion

- unauthorised access to devices

    o unattended devices

    o shoulder surfing

    o theft of device

    o lost devices

    o devices/interfaces installed in public areas

A1.3 Impact of a credible threat, likely to result in some form of loss:

A1.3.1 operational loss

- manufacturing output

- service availability

- data availability

A1.3.2 financial loss

- organisational

    o cash flow problems

    o loss of profits

    o increased insurance costs

- compensation

    o refunds to customers

    o payments for compromising customer data/personal information

    o costs of remedial actions such as credit score/identity protection

    o payment for contractual default/inability to provide contracted service/goods

    o discounts/write-offs to retain/regain customers

- legal liability

    o fines

    o penalty payments

    o costs of statutory requirements in investigations

    o legal fees

A1.3.3 reputational loss

- loss of trust
- poor customer reviews
  - on social media
  - on review websites
  - on organisation's own website
- reduced scores on reputation metrics/web sites

A1.3.4 intellectual property loss

- new product design
- testing and development data
- organisational strategy
- trade secrets

A1.4 Cyber security threats vary over time and cyber security organisations provide regular updates on the current and changing threat landscape.

A1.4.1 National Cyber Security Centre (NCSC) UK

- latest threat reports and malware analysis
- news (reports and advisories on recent activity)

A1.4.2 National Institute of Standards and Technology (NIST) USA

- news (reports and advisories on recent activity)

A1.4.3 Open Web Application Security Project (OWASP)

- OWASP Top 10

A2 System vulnerabilities

Students should apply their knowledge and understanding of the different types of systems and their vulnerabilities, tools to assess the vulnerabilities and the risk management measures.

A2.1 Vulnerabilities of different types of computer and/or systems and the different threats they are exposed to.

A2.1.1 network

- firewall ports
  - types
    - assigned/well known, such as port 80 for Hypertext Transfer Protocol (HTTP)
    - registered, used by operating systems, internet services and specific pieces of software
    - dynamic/private, used for private/customised services, temporary needs

- o vulnerabilities
  - – open ports
  - – spoofing
  - – Denial of Service (DoS)
- external storage devices
  - o universal serial bus (USB)/flash drive
  - o SD card
  - o external hard drive
  - o solid state device (SSD)
  - o optical disk and magnetic tape, in the context of backup systems

A2.1.2 organisational

- permissions or privileges
  - o read, write, execute, modify/change
  - o user, administrator, system, group
  - o on files, folders/directories, devices, data structures, services
- password policy
  - o minimum and maximum length
  - o character restrictions
  - o frequency of password reuse
  - o disallow personal names, birthdays etc.
  - o specify a minimum password age
  - o prevent password sharing/multiple logon with same password
- password management
  - o password managers
    - – on an individual device
    - – synchronised between devices
    - – cloud based
    - – to generate passwords
  - o lockout of inactive accounts
  - o effective new user/leaving user process
  - o auto-filling of forms/screens by
    - – browser
    - – dedicated software

A2.1.3 software

- from an untrustworthy source

- software downloads

  o requirement for
    – trusted source
    – Hypertext Transfer Protocol Secure (HTTPS) or lock symbol
    – malware scan, pre-install
    – hash check

  o malicious/deceptive installers

- illegal copies

  o lack of security support/updates

  o backdoors

  o containing malware

- zero-day exploits

  o new threats

  o window of exploitation before fix/patch applied

- data storage and processing software

  o SQL injection

  o poor/no protection on internet-facing data systems

  o design/security flaws in web interfaces

- missing patches/updates

A2.1.4 operating system, Graphical User Interface (GUI) and Command Line Interface (CLI)

- unsupported/out of support versions

- missing patches/updates

- missing/incorrect security settings

A2.1.5 mobile devices reliant on Original Equipment Manufacturers (OEMs) to update system software

A2.1.6 physical

  o theft of equipment/devices containing sensitive data

  o mobile device

  o data storage device

- poor/missing security for restricted areas

A2.1.7 process of how people use the system

- leaks, intentional and accidental

- sharing security details

- flawed security processes

A2.1.8 security implications of cloud computing and of the Internet of Things (IoT) devices

- Cloud computing

  o missing/incorrect/default security settings

  o third party/cloud provider access

  o reliant on third party security

  o data movement outside of the organisation's network/over the internet, risk of interception/theft/tampering

- IoT

  o weak/no encryption on IoT devices/transmissions

  o default passwords

  o lack of patches and updates

  o deployment by non-IT staff

  o flawed/insecure control interfaces

  o poor/no compatibility with network security systems

  o eavesdropping/smart devices always listening/sending voice data

A2.2 Where to find up-to-date sources of information on specific known hardware and software vulnerabilities**.**

A2.2.1 manufacturer's website

A2.2.2 forum/technical help website for IT professionals/cyber security specialists

A2.2.3 third party websites specialising in specific hardware or software

A2.3 Attack vectors

A2.3.1 Wireless

- Wi-Fi, IEEE 802.11 family of standards

- Bluetooth

- Cellular

- satellite link

- Infra Red (IR)

- Near-field communication (NFC)

- Radio-frequency identification (RFID)

A2.3.2 internet connection

- types

  - copper cable

  - optical fibre

  - Wi-Fi

  - cellular/5G

- connection devices

  - modem/router-modem, cable and optical fibre

  - wireless router

  - cellular device/5G router

A2.3.3 internal network access devices

- router

- switch

- wireless access point

A2.4 Types and uses of tools and methods to assess the vulnerabilities in computer systems

A2.4.1 port scanner

A2.4.2 network mapper/system discovery

A2.4.3 registry checker

A2.4.4 website vulnerability scanner

A2.4.5 vulnerability detection and management software

A2.4.6 assessing user vulnerabilities

A2.5 Use of independent third-party review of a system and network designs before implementation

A2.5.1 establishing due diligence

A2.5.2 third party certification

A2.6 Applications and features of penetration testing for common threats, those in the Open Web Application Security Project (OWASP) top 10.

A2.6.1 uses range of techniques to find weak spots

A2.6.2 checks against lists of known vulnerabilities

A2.6.3 produce reports, in appropriate formats

A2.7 Passive risk management measures:

A2.7.1 risk transfer to a third party (commissioning a service provider)

A2.7.2 risk avoidance by stopping an activity

A2.7.3 risk acceptance

A3 Legal responsibilities

Students should know the responsibilities in relation to current legal legislation.

A3.1 Current legislation

A3.1.1 General Data Protection Regulation (GDPR) (requirements for protection of data, privacy rights)

A3.1.2 Computer Misuse Act 1990 (protects personal data held by organisations from unauthorised access and modification).

A3.2 Areas the legislation applies to

A3.2.1 protection of data, in storage and when transferred

A3.2.2 privacy, personally identifying information (PII)

A3.2.3 unauthorised access to computers/devices

A3.2.4 unauthorised access to and modification of data

A3.3 Legal responsibilities legislation

A3.3.1 General Data Protection Regulation (GDPR)

- principles
  - lawfulness
  - fairness and transparency
  - limited to stated purpose(es)
  - accuracy
  - keep minimum amount of data
  - store for minimum amount of time
  - maintain confidentiality and integrity
- legal reasons for data processing
  - consent
  - contractual obligation
  - legitimate interest
  - vital interest
  - legal requirement
  - public interest
- personal rights, people have the right to:
  - access their own personal data
  - be informed about how and why their data is used
  - have their data corrected, removed or restricted
  - object to the data being used

- o portability (have data supplied in a machine readable format)
- o not to be subject to a decision based solely on automated processing.
- Computer Misuse Act
- o responsibilities of organisations – exercise due care to comply with its security obligations under GDPR

A4 Software and hardware security measures

Students should apply their knowledge and understanding of the use and effectiveness of security measures for software and hardware, use of encryption and precautions to protect wireless local area network (WLAN)

A4.1 Software and hardware

A4.1.1 physical security measures

- site security locks
  - o mechanical
  - o electronic
  - o network connected
- card entry
  - o Near-field Communication (NFC)
  - o Radio-frequency Identification (RFID)
  - o barcode, QR code
  - o magnetic stripe
  - o embedded microprocessor/chip
- biometrics
  - o fingerprint
  - o iris/retina/eye pattern
  - o facial recognition
  - o voice recognition
  - o handwriting/signature/pattern, etc. – on touchscreen/pad
- Closed-Circuit Television (CCTV)
- security staff
- alarms – on buildings/restricted areas and on devices
- protected cabling and cabinets
- staff training

A4.1.2   data storage, data protection and backup, and recovery procedures

- backup types
  - full
  - differential
  - incremental
- backup strategies
  - onsite, offsite, cloud
  - automated, manual
  - hot site, warm site
- redundant array of independent disks (RAID) vs backup
- archiving vs backup
- data resilience
- recovery types
  - file/data restore
  - image restore of; disc, device, system
  - full/bare-metal restore

A4.1.3   antivirus software and detection techniques

- virus signatures, scanning
- heuristics techniques used to identify potentially suspicious file content or behaviour
- file integrity check, checksum
- techniques for dealing with identified threats
  - warning
  - logging
  - prevent execution
  - quarantine
  - deletion

A4.1.4   software and hardware firewalls and the filtering techniques they use

- packet filtering and inspection
- application layer awareness
- inbound and outbound rules
- network address

A4.1.5   user authentication

- user login procedures

- strong password, password policy compliance

- biometric authentication

- single factor and multi-factor authentication (MFA)

  o knowledge/things you know

  o possession/things you have

  o inherence/things you are

  o location factors such as IP address, MAC address, global positioning system (GPS) location

  o behaviour factors such as how a signature/pattern is made, how a keyboard is used

- security tokens

  o connected such as a Universal Serial Bus (USB) key, or smartcard plus reader

  o contactless such as a Bluetooth enabled dongle

  o disconnected, a device that generates a code independently such as:
    - a smartphone with a security app
    - a dedicated device issued by a bank or credit card company

- Kerberos network authentication for Windows® and Linux®-based operating systems

- basic key exchange process

  o client request

  o server response

  o authentication of server response

  o key exchange

- certificate-based authentication

  o Transport Layer Security (TLS)

  o Secure Sockets Layer (SSL)

  o client/device certificate

  o Public Key Infrastructure (PKI)

  o Certificate Authority (CA)

  o self-signed certificate

A4.1.6 access controls and the methods to restrict users' access to resources

- Discretionary Access Control (DAC), users have control of their own files and resources

- Role-Based Access Control (RBAC), administrator sets rules groups of users based on their role in an organisation

- Rule-Based Access Control (RBAC), administrator sets rules for individual users

- resources

    o applications

    o folders

    o files

    o data sets

    o physical resources/devices

A4.1.7 trusted computing

- benefits, increased security

- drawbacks, loss of user control/privacy/anonymity

A4.1.8 Finding lost or stolen devices

- device location technology

    o Global Positioning System (GPS)

    o phone home on connection

    o device tracking and location reporting software

A4.1.9 Device based security

- timed lockout of desktop/screen

- desktop/screen lock after failed login attempts

- memory wipe/factory reset after failed login attempts

- remote access for lock/wipe/reset of lost/stolen device

A4.2 Use of encryption

A4.2.1 storage encryption

- safe password storage

- Digital Rights Management (DRM)

- file, folder, disc, device encryption

A4.2.2 communications encryption

- symmetric encryption
  - secret key
  - Advanced Encryption Standard (AES)
- asymmetric encryption
  - public and private keys
  - Rivest–Shamir–Adleman (RSA)
  - Diffie–Hellman key exchange
- integrated into smart, mobile and built-in/embedded devices
- The Onion Router (TOR)
- Virtual Private Networks (VPNs)
- digital certificates and certificate authorities
- Hypertext Transfer Protocol Secure (HTTPS)
- public/private keys
- End-to-End Encryption (E2EE)
- secure message apps

A4.3 Precautions that can be taken to protect a Wireless Local Area Network (WLAN) from unauthorised access:

A4.3.1 Media Access Control (MAC) address filtering and hiding the Service Set Identifier (SSID)

A4.3.2 wireless encryption

- Wi-Fi Protected Access 2 and 3 (WPA2/3)
- Wi-Fi Protected Setup
- known wireless vulnerabilities
  - unsecured access point
  - piggybacking/unauthorised use of unsecured network
  - Evil Twin attack/fake access point
  - wireless sniffing/eavesdropping
- mitigation methods for attacks on Wi-Fi
  - changing default passwords/settings/names
  - use of block and allow lists for device access
  - use of VPNs
  - use of WPA2/3
  - firewalls

A4.4 Security issues during network and system design to ensure security is built

A4.4.1 expect attacks to happen and plan for them

A4.4.2 design the system to run on 'fewest privileges'

A4.4.3 assume everyone will get access to the system design

A4.4.4 avoid reliance on secrecy/obscurity

A4.4.5 compliance with information security standards such as ISO 27000

B: Use of networking architectures and principles for security

Students should apply their knowledge and understanding of the security issues of networked systems and how to secure them in organisational contexts. Students should be able to interpret and amend schematic diagrams.

B1 Network types

B1.1 Applications and features of networks:

B1.1.1 Network types

- Local Area Network (LAN)
- Wireless Local Area Network (WLAN)
- Wide Area Network (WAN)
- Storage Area Network (SAN)
- Personal Area Network (PAN)
- the internet

B1.1.2 Private network types

- intranet
- extranet
- cloud network

B1.1.3 wired and wireless integration

- ethernet standards for wired and wireless (802 family)
- compatibility/interoperability issues such as protocols and access points
- admin issues such as channels and IP addresses
- technical issues such as signal strength and interference

B1.1.4 schematic diagrams

- network diagram, logical and physical
- diagrams showing specific items such as port numbers or network addresses

B1.1.5 Features/requirements of networks (cyber security related)

- scalability
- software and hardware sharing/compatibility
- data and file sharing/transfer
- performance/response time
- backup management
- security settings
- reliability
- fault tolerance
- communications

B1.2 Applications and features of network topologies:

B1.2.1 physical topologies

- star
- extended star
- hierarchical
- wireless mesh
- ad-hoc (mix of wired and wireless for Bring Your Own Device (BYOD))

B1.2.2 logical topologies

- logical bus
- logical ring

B1.3 network architecture

B1.3.1 peer-to-peer

B1.3.2 client/server

B1.3.3 thin client

B1.4 modern trends – applications and security issues of:

B1.4.1 virtualisation

- segmentation
- isolation/sandboxing/containerisation
- reduced attack surface

B1.4.2 cloud computing

- configuration issues, default access settings

- reliance on service provider, data leaks/loss/theft

- Application Programming Interfaces (API), vulnerabilities in interface to cloud services/storage

- account hijacking

B1.4.3 BYOD

- issues with organisational data on a private device

  o password policy

  o owner's/organisation's privacy

  o data security, on device and when transferred

  o patches, maintenance, updates, compatibility

  o organisational v personal applications

  o erasing/wiping data after use/when no longer required

  o tracing/auditing data use/movement

- Software-Defined Networking (SDN)

  o segmentation

  o remote management

  o automation

  o scalability

  o reduced hardware requirements

- Storage Area Network (SAN)

  o redundancy

  o scalability

  o access controls

  o encryption/digital certificates

- Internet of Things (IoT)

  o Application Program Interface (API) security issues

  o default passwords/security settings

  o lack of patches/updates

- o Zigbee, Bluetooth 5 and similar low-power wireless technology
  - – mesh capability
  - – ease of interception/interference
  - – range issues
- o botnets
- o spying via networked cameras/smart hubs/TVs
- o exposure of non-traditional networked devices such as medical equipment, home appliances, commercial machinery, and vehicles

- remote working
  - o devices seen/used by others such as family members, visitors
  - o need for VPN/encrypted link
  - o security of home network/Wi-Fi
  - o weaknesses of/reliance on third party communication systems such as video calls
  - o issues around data storage/transfer/use of the cloud

B2 Network components

B2.1 Application and features of hardware components:

B2.1.1 end-user devices, with connectivity and processing

- mobile devices
  - o mobile phone/smartphone
  - o laptop/netbook/notebook
  - o tablet
  - o handheld game console and other entertainment devices
  - o smartwatches and fitness trackers
  - o digital cameras
  - o virtual reality and augmented reality sets
- fixed, networked devices with processing and/or storage
  - o server
  - o Personal Computer (PC)/workstation
  - o printer
  - o scanner
  - o Network Attached Storage (NAS)
  - o multi-functional devices (any combination of devices in B2.1.1)

B2.1.2   connectivity devices

- switch, managed and unmanaged
- router, wired and wireless
- gateway
- bridge
- repeater
- access point
- USB hub, active and passive
- modem
    - Digital Subscriber Line (DSL)/copper cable
    - optical fibre modem
    - wireless modem
- multi-functional devices (any combination of devices in B2.1.2)

B2.1.3   connection media

- cable
    - Ethernet
    - universal serial bus (USB), current types and legacy requirements
- Wireless
    - Wi-Fi, IEEE 802.11 family of standards
    - NFC
    - Bluetooth, current types and legacy requirements
    - cellular, 5G
- optical fibre
- Li-Fi

B2.2 Application and security issues of external media and storage

B2.2.1   encryption

B2.2.2   secure disposal

B2.2.3   loss/theft of media

B2.2.4   interception/copying

B2.2.5   data loss/corruption

B2.2.6   media lifespan/failure

B2.2.7   malware vector

B2.3 Application and features of software components

B2.3.1 network and device operating systems

- Graphical User Interface (GUI)
- Command Line Interface (CLI)
- web interface, internal web page for device control/configuration

B2.3.2 network monitoring, management and troubleshooting tools

- remote access administration tools
- performance monitor
- events and logs viewer
- vulnerability scanner
- network analyser/packet sniffer

B2.3.3 network applications

- remote working tools
- database
- document management
- network discovery/mapping tools.

B3 Networking infrastructure services and resources

B3.1 Application and function of:

B3.1.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

- four layer model
- Transport Layer Security (TLS)
- packets and headers
- error correction

B3.1.2 ports

- hardware, switch ports
- software/virtual, Internet Protocol ports

B3.1.3 packet

- header
- trailer/footer
- payload/body/content
- types
  - o Transmission Control Protocol (TCP)
  - o Internet Protocol (IP)
  - o User Datagram Protocol (UDP)

B3.1.4 network address translation (NAT)

- types
  - static
  - dynamic
  - Port Address Translation (PAT)
- structure and format of IPv4 and IPv6 addressing
- RFC 1918 private addresses
  - Class A: 10.0. 0.0 to 10.255. 255.255
  - Class B: 172.16. 0.0 to 172.31. 255.255
  - Class C: 192.168. 0.0 to 192.168. 255.255
  - Automatic Private IP Addressing (APIPA) for DHCP failure, 169.254.0.1to 169.254.254.255
  - reserved IP addresses such as 127.0.0.1 loopback address

B3.2 Application of domains, sub-domains and segmentation

B3.2.1 hierarchy

B3.2.2 trust relationships

B3.3.3 access control

B3.3.4 security benefits

- limits access to devices, data, and applications
- restricts lateral movement of attack/malware/intruder
- smaller attack surface
- simpler damage control

B3.3 Application of network devices to configure networks

B3.3.1 server

B3.3.2 router

B3.3.3 switch

B3.3.4 Wireless Access Point (WAP)

B3.3.5 firewall

B3.3.6 bridge

B3.3.7 gateway

B3.4 Application and function of network infrastructure services

B3.4.1 Domain Name System (DNS)

- DNS resolution process

- reverse DNS resolution

- DNS cache

- IPv6 DNS

B3.4.2 directory services (DS), identity and access management

- active directory

- open directory

- OpenLDAP

B3.4.3 authentication services

- types
  - single-factor
  - two-factor (TFA)
  - multi-factor (MFA)
  - single sign on (SSO)

- authentication protocols
  - Password Authentication Protocol (PAP), (RFC 1334)
  - Challenge Handshake Authentication Protocol (CHAP), (RFC 1994)
  - Extensible Authentication Protocol (EAP), (RFC 5247)

B3.4.4 Dynamic Host Configuration Protocol (DHCP)

- DHCP servers and clients

- IP address allocation process

- basic configuration settings
  - address ranges
  - lease information
  - reservations/static addresses
  - dynamic addresses/allocation
  - automatic addresses/allocation
  - server address

B3.4.5 routing

- static

- dynamic/adaptive

- routing tables

- Interior Gateway Protocols (IGPs), within one network/organisation

- Exterior Gateway Protocols (EGPs), between networks

- Border Gateway Protocol (BGP), internet routing

B3.4.6 remote access services

- by dial-up, using telecommunications services

- by VPN, over the internet

- handshake/connection processes, client-host/server

- uses/gives access to

  o devices

  o files

  o data

  o desktops

  o applications

B3.5 Application and function of network services and resources

B3.5.1 file and print services

- file server, networked file storage

- print server, networked printer

- file management, tracking, sharing

- print management, sharing, queueing, prioritising

- printer configuration and driver management

B3.5.2 web, mail and communications services

- web services

  o use HTTP or HTTPS protocols

  o use XML messaging system

  o are independent of operating system or programming language

  o allow applications to communicate

  o allow sharing of data, functionality

- mail services

  - use *Simple Mail Transfer Protocol* (SMTP), *Post Office Protocol* (POP), and *Multipurpose Internet Mail Extensions* (MIME)

  - protocols lack built-in encryption

  - mail server and client

  - process of finding destination server for mail delivery

  - communications services

  - email

  - Voice over IP (VoIP)/Internet Calling

  - SMS/text Messaging

  - video conferencing

  - social networking applications

  - online collaboration tools

  - Communication as a Service (CaaS)

C: Cyber security documentation

Students should know and understand the governance policies and documents needed to establish and maintain security on an ongoing basis.

C1 Internal policies

General IT policies

C1.1   Use of general security-related IT policies and their effectiveness

  C1.1.1   a cyber security policy that uses the Plan-Do-Check-Act loop derived from part of the International Organization for Standardization (ISO) 27001:2013

  - policies on internet and email use

    - inappropriate, offensive, illegal material

    - sending confidential information

    - privacy issues

    - upload/download of copyrighted material, music, video

    - download of executable files

    - visiting potentially dangerous websites

    - organisations rights and obligations to scan traffic, monitor activities, retain copies of emails, etc.

- security and password procedures
  - length/strength policy
  - management and enforcement tools
  - deny lists of common/weak passwords
  - monitoring/logging of password attempts
  - lockout policy for inactivity, login attempts
  - use of technology to reduce requirement for passwords
- staff responsibilities
  - complete required security training
  - follow security procedures and report problems
  - respond to/report suspicious activity
  - maintain security in own workspace/behaviour
- staff IT security training
  - leadership/management to ensure training is staffed/funded/resourced
  - flexibility of training program so everyone can take part
  - range of training resources/learning styles
  - progress tracking
  - incentives rather than punishment
  - ongoing training for reinforcement and for new threats

C1.1.2 security audits and their application to check compliance against policies

- audit goals and scope
- identify problems/gaps/weaknesses
- check against internal policies
- check against external regulations/laws
- reporting of results, required improvements/changes

C1.1.3 backup policy

- selection of data
- backup methods
- backup type
- frequency/scheduling
- storage strategy
- responsibility, accountability
- backup testing strategy

- legal/regulatory compliance
- emergency/recovery procedures

C1.1.4 data protection policy to ensure organisational compliance

- Data Protection Officer
- follow data protection principles
- protecting rights/privacy
- staff training
- system security procedures
- application of policy to external contractors/consultants/vendors etc.
- responsibility and accountability of staff/organisation

C1.1.5 cyber security incident response policy

- contacts
  - incident response team leader/provider
  - IT team leader/provider
  - senior management
  - legal
  - public relations
  - human resources
  - insurance
- procedures/flowcharts/checklists for
  - initial decisions/triage/escalation
  - main response, analysis, containment, mitigation, recovery
  - reviewing, reporting, closing the incident
- communications
  - contact telephone plus alternative/backup
  - conference call facility

C1.1.6 disaster recovery policy

- purpose and scope
- triage, a list of possible events, their severity and appropriate response
  - activate cyber security incident response
  - activate business continuity plan
  - activate disaster recovery plan
- roles, responsibilities

- contact lists
- monitoring and reporting requirements

C1.1.7 external services policy

- general for external services policies
  - authorization and access control
  - management, responsibility, accountability
  - contact details
  - regulatory compliance
  - incident response procedures
- cloud
  - cloud resources requiring protection
  - acceptable use
  - data protection
- hardware
  - sources, vendors, contractors, other third parties
  - service agreements
  - maintenance and support
- software
  - sources, vendors, contractors, other third parties
  - service agreements
  - licencing
  - software support
- support
  - service time/availability
  - response time – report to support starting
  - troubleshooting/completion/solution time, time to fix the problem
  - escalation procedures

D: Forensic procedures

D1 Forensic collection of evidence

Students should apply their knowledge and understanding of the methods for collecting forensic evidence following a security incident

D1.1 Forensics on devices – servers, PCs and mobile devices

D1.1.1 meeting requirements for forensics

- confiscation of devices
  - prior planning for a range of devices/scenarios
  - passwords, codes, PINs, etc.
  - chargers, cables etc. for mobile devices
  - retain current power state/status if possible
  - isolation of device from network/communications (if device is suspected to be communicating)
    - photograph screen
    - turn off device
    - remove battery/power cable
    - use airplane mode
    - disable wireless communication
    - use Faraday bag/cage
  - appropriate packaging
  - document chain of custody
  - establish legal permissions
- taking an image of the system
- using a forensic analysis tool
- reviewing files and settings
- reviewing system logs
- reviewing user activity
- malware analysis and alerts

D1.1.2 the challenges of live forensics

- changing data in situ
- recovering corrupted data and preventing data corruption
- capturing data in active memory
- capturing remote data
- not losing temporary files

D1.1.3 network forensics

- agreeing a network-testing forensics methodology with supervisory and investigatory authorities
- scanning of local infrastructure
  - o ensuring permission is granted
  - o ensuring that testing protocol will not disrupt a live system
  - o passive and active analysis tools
- reviewing and analysing firewalls and infrastructure devices
  - o switch
  - o router
  - o Wireless Access Point (WAP)
  - o client or server logs
- analysing malware activity and alerts

D1.1.4 Documenting the scene

- prior planning for a range of scenarios
- securing the scene
- plans, photos, diagrams of the scene
- contemporaneous notes
- witness statements

D2 Systematic forensic analysis of a suspect system

Students should apply their knowledge and understanding of the requirements and processes for forensic analysis

D2.1 Requirements for maintaining an accurate record, made at the time, or as soon after the incident as possible

D2.1.1 Retaining snapshots of the system

- originals/clean system for comparison
- generate hash function/checksum for copies/images
- whole disk/machine, with/without 'boot' facility
- files/folders directories/data structures
- memory, RAM, BIOS, memory cards/SIM
- virtual discs/machines
- process/sub-process output/activity
- network information such as open ports, IP addresses, user logins

- temporary files, deleted data

- system generated data such as System Volume Information, hibernation files, shadow copies, crash dumps, page files, synchronisation files

D2.1.2 Requirements for the recording of all findings and considering how reliable the evidence is

- no collection/action that could change data on a digital device

- collection by competent person

- creation of trail or record of all actions taken, chain of custody

- documentation of who is responsible for collection/decisions/enforcement of standards

D2.1.3 Requirements for the recording of any alterations that have been intentionally and unintentionally imposed by the investigator

- documentation of all actions from initial seizure

- potential inadmissibility of altered data

- working with copies/images rather than original data/device

D2.1.4 Requirements for the creation of visual evidence of findings

- photos, videos

- screenshots

- data-time stamps. metadata

D2.1.5 Ensuring the evidence is relevant and not a false positive

- defining file signatures, search criteria, etc.

- known/estimated error rates of tools/target data types

- feedback of false positive data to improve detection method/algorithm

- alert fatigue for high false positive rates

- manual review of all positives to filter obvious false ones

- further investigation/check of filtered positives

D2.2 Assessing the findings to determine whether or not they:

D2.2.1 provide evidence of a crime and/or an incident

- criminal

- regulatory breach

- civil liability, contractual breach

- non-compliance with internal policy

- cyber attack

- negligence, mismanagement, etc.

D2.2.2 show that the system has been externally and/or internally compromised

- unusual traffic
  - inbound
  - outbound
  - from unusual geographical regions
  - DoS/DDoS signs
- unusual login attempts
- unusual DNS requests
- increase in file/data reads
- increase in file/data requests
- unusual port usage
- suspicious changes to files/data
- suspicious access to/changes to system files/data

D2.3 Writing security reports on

D2.3.1 actions to prevent security incidents from reoccurring in the future

- general report structure
  - title
  - contents
  - introduction
  - headings and sub-headings
  - consistent use of bullets and numbering
  - conclusions
  - footnotes
  - citations
- analysis of the incident to identify
  - errors/omissions in procedures
  - unforeseen problems
  - errors/omissions in preventative measures
  - errors/ delays in detection/alerting
  - remedial actions

D2.3.2 improvements to the content of IT policies

D2.3.3 improvements to security protection measures

- physical

- software

- hardware

- processes and procedures

- training

Transferable skills

Managing Yourself	Effective Learning	Interpersonal Skills	Solving Problems
MY – TPR	EL – MOL	IS – WC	SP – CT *
MY – PS&R	EL – CL	IS – V&NC	SP – PS
MY – COP	EL – SRS	IS – T	SP – C&I
MY – PGS	EL-PRS	IS – C&SI	

Table key

*	Signposted to indicate opportunities for development as part of wider teaching and learning.
√	Embedded in teaching, learning and assessment
blank	TS not embedded or signposted in unit

Key terms typically used in assessment

The following table shows the key terms that will be used consistently by Pearson in our assessments to ensure students are rewarded for demonstrating the necessary skills.

Please note: the list below will not necessarily be used in every paper/session and is provided for guidance only.

Command or term	Definition
Complete	Students add or amend a diagram or process. Can apply to problems/solutions of varying complexity.
Describe	Students provide an account of something or highlight several key features of a given topic. May also be used in relation to the stages of a process.
Explain	Students identify a point and give a linked justification/exemplification of that point. The answer must contain some linked reasoning.
Evaluate	Students consider various aspects of a subject's qualities in relation to its context such as: strengths or weaknesses, advantages or disadvantages. They come to a judgement supported by evidence which will often be in the form of a conclusion.
Identify	Students select some key information from a given stimulus/resource.
State, name, give	Students recall one or more pieces of information

Unit 3: Website Development

Level: 3

Unit type: Internal

Guided learning hours: 60

Unit in brief

Students will investigate fundamental principles in website development. They will design and develop a website in response to a client brief.

Unit introduction

Website development skills are more essential than ever if you want to be noticed, reach your goals and generate interest in today's sophisticated, competitive and dynamic online environment. Modern lifestyles are digitally driven and as a website developer you must combine different tools and techniques to capture and maintain the user's interest. Website developers need to understand and acquire the necessary skills to find solutions to a variety of scenarios and problems.

In this unit, you will explore how existing websites use the principles of website development to appeal to their intended audience and meet their specific purpose. You will plan, design and develop a website in response to a client brief by applying website development tools, techniques and processes. You will also reflect on the usability, functionality and fitness for purpose of the website using a testing and review process.

Many software developers, database experts and systems managers need web-client development skills as an integral part of their overall portfolio of expertise. This unit will benefit you to progress on to information technology courses in higher education.

Learning aims

In this unit you will:

A Understand how the principles of website development are used to create effective websites.

B Explore website design skills and techniques to meet client requirements.

C Develop a website to meet client requirements.

Summary of unit

Learning aim	Key content areas	Assessment approach
A Understand how the principles of website development are used to create effective websites	**A1** Purpose and principles of websites **A2** Planning a website in response to a client brief	Pearson-Set Assignment Brief Task 1: Conduct research to analyse how the principles of website development are used to meet a specific purpose and develop ideas and plans to meet a client's requirements.
B Explore website design skills and techniques to meet client requirements	**B1** Website design **B2** Asset management techniques	Pearson-Set Assignment Brief Task 2: Produce designs and assets for a website to meet a client's requirements.
C Develop a website to meet client requirements	**C1** Common tools and techniques to produce a website **C2** Website development processes **C3** Testing	Pearson-Set Assignment Brief Task 3: Develop a website to meet a client's requirements.

Content

The essential content is set out under content areas. Students must cover all specified content before the assessment.

Learning aim A: Understand how the principles of website development are used to create effective websites [EL-SRS]

A1 Purpose and principles of websites

- Purpose and audience:
  - o purpose of websites, to include:
    - eCommerce
    - to provide information
    - to promote products or services
    - to provide entertainment
  - o target audience, to include:
    - demographics
    - user personas.
- Principles of website development:
  - o page layout, to include:
    - F-Shaped pattern
    - Z-shaped pattern
    - grid layout
    - visual hierarchy
    - grouping elements
    - separating content
    - unconventional layouts
  - o navigation, to include:
    - fixed/sticky navigation bars
    - vertical navigation
    - hamburger menu
    - logical navigation
  - o content, to include:
    - written content
    - visual content
    - calls-to-action
  - o design, to include:
    - typography
    - colour scheme

- o user experience:
  - accessibility, to include:
    - colour contrast
    - colour combinations
    - closed captions, transcripts
    - keyboard-only navigation
    - breadcrumbs
    - customisable features
  - consistency, to include:
    - branding
    - page layout
    - design
    - User Interface (UI) elements
  - user-friendly, to include:
    - simplicity
    - intuitive
    - engaging
    - responsive
  - use of motion and movement, to include:
    - micro-interactions
    - animation
    - parallax scrolling
    - image sliders
    - purpose of motion
- o dynamic websites, to include:
  - customised user experience
  - controlled access to content
- o cross-browser compatibility, to include:
  - reducing discrepancies in different browsers
  - mobile compatibility
- o search engine optimisation.

A2 Planning a website in response to a client brief

- Establishing the client's requirements:
  - o purpose, to include:
    - problem to be solved
    - key messages
    - user motivations and goals
  - o intended audience
  - o technical requirements

- Research to identify new ideas:
  - existing websites
  - content ideas
  - available resources
  - legal and ethical constraints:
    - copyright
    - data protection
    - digital accessibility
    - inclusive and diverse content and representations
- Structuring the website:
  - site map:
    - number of pages
    - content and features
    - site navigation.

Learning aim B: Explore website design skills and techniques to meet client requirements

B1 Website design

- Creating wireframes:
  - wireframing tools, to include:
    - sketching on paper
    - graphic design software
    - UX design software
    - wireframing app
  - wireframing techniques, to include:
    - hierarchy of page elements
    - balance of content
    - grouping elements
    - aligning elements
    - accurate dimensions.
- Design ideas:
  - visual style, to include:
    - colour palette
    - branding
    - typography

- Reviewing fitness for purpose:
  - quality, to include:
    - clarity
    - detail
  - user experience
  - meeting client requirements.

B2 Asset management techniques

- Creating assets:
  - writing headlines and copy, to include:
    - short sentences
    - short paragraphs
    - avoiding jargon
    - appropriate mode of address
  - visual assets, to include:
    - image editing techniques
    - image manipulation techniques
    - vector graphic drawing techniques.
- Sourcing assets, to include:
  - written copy
  - stock images
  - icons
  - video.
- Preparing assets, to include:
  - trimming video
  - compression
  - file formats.
- Managing assets, to include:
  - logical folder structure
  - naming conventions.

Learning aim C: Develop a website to meet client requirements [MY-TPR]

C1 Common tools and techniques to produce a website

- Hypertext Markup Language (HTML):
  - navigation, to include:
    - menus
    - internal and external links
    - anchors

- o adding content, to include:
    - – text
    - – images
    - – video
    - – tables of information
  - o forms.
- Cascading Style Sheets (CSS):
  - o styling, to include:
    - – colour
    - – web typography
    - – text formatting
    - – links and buttons
    - – tables
    - – forms
  - o page layout, to include:
    - – CSS box model
    - – responsive layouts, to include:
      - ▪ CSS media queries
      - ▪ layout tools.
- Function of JavaScript in website development, to include:
  - o displaying images:
    - – sliders
    - – gallery
  - o displaying information:
    - – accordion
    - – tabs
    - – modal box
    - – filtering information
  - o animation:
    - – hover effects
    - – transitions
    - – animated logo
    - – motion
  - o search functionality
  - o shopping cart
  - o interactive maps
  - o video, to include:
    - – controlling video
    - – video backgrounds.

C2 Website development processes

- Accessibility:
  - features, to include:
    - alternative tags
    - zoom features
    - text-to-speech
  - standards, to include:
    - Web Content Accessibility Guidelines (WCAG)
    - World Wide Web Consortium (W3C) standards
    - HTML5 standards
  - semantic HTML.
- Consideration of search engine optimisation.
- Self-review:
  - areas for consideration:
    - quality in comparison to similar websites
    - suitability for audience and purpose
    - meeting client requirements
    - legal and ethical constraints
    - consistency
    - readability
- Publishing the website.

C3 Testing

- Functionality testing:
  - test plan
  - areas, to include:
    - links
    - user interactivity
    - responsive to different screen sizes.
- Usability testing:
  - user testing audit
  - areas, to include:
    - accessibility
    - logical navigation
    - clarity of information
    - user experience.

Assessment criteria

Learning aim A: Understand how the principles of website development are used to create effective websites

Pass	Merit	Distinction
A.P1 Undertake research which shows adequate understanding of how the principles of website development are used to meet a specific purpose, using partially relevant examples. **A.P2** Produce a site map that partially meets the client's requirements.	**A.M1** Undertake research which shows a good understanding of how the principles of website development are used to meet a specific purpose, using mostly relevant examples. **A.M2** Produce a site map that mostly meets the client's requirements.	**A.D1** Carry out effective research to demonstrate a thorough understanding of the principles of website development and how to comprehensively meet the client's requirements, using pertinent examples.

Learning aim B: Explore website design skills and techniques to meet client requirements

Pass	Merit	Distinction
B.P3 Produce adequate wireframes and visual designs for a specific purpose. **[SP-C&I]** **B.P4** Use asset management techniques to develop assets that partially meet the client's requirements. **[SP-C&I]**	**B.M3** Produce mostly effective wireframes and visual designs for a specific purpose. **B.M4** Use asset management techniques to develop assets that meet most of the client's requirements.	**B.D2** Make effective use of website design skills to develop designs and assets that comprehensively meet the client's requirements.

Learning aim C: Develop a website to meet client requirements

Pass	Merit	Distinction
C.P5 Use tools, techniques, processes and testing to produce a website that partially meets the client's requirements. **[SP-C&I]**	**C.M5** Use tools, techniques, processes and testing to produce a website that meets most of the client's requirements.	**C.D3** Use tools, techniques, processes and testing to produce a website that comprehensively meets the client's requirements.

Transferable skills

Managing Yourself	Effective Learning	Interpersonal Skills	Solving Problems
MY – TPR *	EL – MOL	IS – WC	SP – CT
MY – PS&R	EL – CL	IS – VC	SP – PS
MY – COP	EL – SRS *	IS – T	SP-C&I √
MY – PGS	EL-PRS	IS– C&SI	

Table key

*	Signposted to indicate opportunities for development as part of wider teaching and learning.
√	Embedded in teaching, learning and assessment
blank	TS not embedded or signposted in unit

Essential information for Pearson Set Assignment Briefs (PSAB)

Pearson sets the assignment for the assessment of this unit.

The PSAB will take 15 hours to complete.

The PSAB will be marked by centres and verified by Pearson.

The PSAB will be valid for the lifetime of this qualification.

Assessing the PSAB

You will make assessment decisions for the PSAB using the assessment criteria provided.

Section 1 gives information on PSABs and there is further information on our website.

Further information for teachers and assessors

Resource requirements

For this unit, students must have access to resources that will enable them to develop the skills and techniques to design and develop websites, including:

- wireframing tools
- software and apps to create visual styles and visual representations
- equipment and software to create and prepare assets
- software tools to develop a website.

The website does not need to include a payment system.

The choice of tool can be made by centres. There are three considerations, which are as follows:

- Can you be sure that the work done is that of the student (Cloud services can be accessed at any time by anyone and so there may be doubt about who really created the evidence)?
- Can every student evidence all assessment criteria (the tool must not be functionally limiting in any way)?
- Can the evidence be produced in a format that is accessible to your Standards Verifier (it is worth checking with your Standards Verifier early if the evidence will be in an unusual format)?

Essential information for assessment decisions

Learning aim A

For distinction standard, students will show a thorough understanding of how different websites combine principles of website development to meet their purpose. Students will also analyse the impact of the use of these principles on the user. Students will draw on pertinent examples and consider positive and negative outcomes.

Students will conduct accomplished research to underpin their planning, including effective research into existing websites, possible content for the website and legal and ethical constraints. A detailed site map will be annotated to clearly show how the proposed website will meet the client requirements.

The response will be considered and well-structured and relevant technical vocabulary will be used accurately.

For merit standard, students will show good understanding of how different websites employ principles of website development to meet their purpose. Students will also explain the impact of the use of these principles on the user. Understanding will be supported by some mostly relevant examples from the chosen websites.

Students will conduct mostly effective research to underpin their planning, including relevant research into existing websites, possible content for the website and legal and ethical constraints. A site map will be annotated to show how the proposed website will meet most of the client requirements.

The response will have an appropriate structure and some relevant technical vocabulary will be used.

For pass standard, students will show adequate understanding of how different websites employ some principles of website development to meet their purpose. Understanding will be supported by some partially relevant examples from the chosen websites.

Students will conduct adequate research to underpin their planning, including some research into existing websites, possible content for the website and legal and/or ethical constraints. A site map will show how the proposed website will meet some of the client requirements.

The response will be detailed, although it may lack a coherent structure and it may include some inaccuracies.

Learning aim B

For distinction standard, students will make accomplished use of wireframing tools and techniques to produce effective wireframes. Effective designs for the visual style of the website and representations of the web pages will demonstrate thorough understanding of the client's requirements and user needs.

Assets will be created, sourced and prepared through effective use of asset management techniques. The assets will have clear audience appeal and will comprehensively meet the client's requirements.

For merit standard, students will make good use of wireframing tools and techniques to produce mostly effective wireframes, successfully achieving the result for the specific purpose. Appropriate designs for the visual style of the website and representations of the web pages will demonstrate good understanding of the client's requirements and user needs.

Assets will be created and sourced through good use of asset management techniques. The assets will have appropriate audience appeal and meet most of the client's requirements, although one or two requirements may be missed.

For pass standard, students will make basic use of wireframing tools and techniques to produce adequate wireframes. Straightforward designs for the visual style of the website and representations of the web pages will demonstrate partial understanding of the client's requirements.

Assets will be created and sourced through basic use of asset management techniques. The assets will have some appropriate audience appeal and will meet the key requirements of the client but will not meet other requirements of the client.

Learning aim C

Students are expected to make appropriate use of online tools, techniques and processes to produce a website in response to a Pearson Set Assignment Brief. This includes the use of artificial intelligence (AI), such as AI tools in web development software, website builders, online code generators and generative AI.

The unit encourages student-led creativity, supported by use of new and emerging technologies, including generative AI. However, any use of AI tools and technologies must be explained by students. This could be through annotated screen shots or narrated screen recordings.

For distinction standard, students will make creative use of tools and techniques to build a website that meets all of the client's requirements. Effective understanding of web standards will be demonstrated through the development of a consistent and accessible website.

Students will conduct effective functionality and usability testing. Students will use the outcomes of the testing and a thorough self-review of their website to make considered refinements to the final website.

For merit standard, students will make good use of tools and techniques to build a website that meets most of the client's requirements, although one or two minor requirements may be missed. Students will demonstrate good understanding of web standards through the appropriate use of accessibility features that clearly meet the requirements of the brief.

Students will conduct appropriate functionality and usability testing. Students will use the outcomes of the testing and a self-review of their website to make appropriate refinements to the final website.

For pass standard, students will make basic use of tools and techniques to build a website that meets the key requirements of the client but will not meet other requirements of the client. The website will be functional, although there may be some performance issues.

Students will provide evidence of straightforward functionality and usability testing. Students will use the outcomes of the testing and a self-review of their website to refine the final website.

Links to other units

This assessment for this unit allows students to draw on knowledge, understanding and skills developed from: *Unit 1: Information Technology Systems.*

Unit 4: Relational Database Development

Level: 3

Unit type: Internal

Guided learning hours: 60

Unit in brief

Students will examine relational database development principles to understand the importance of data storage and normalisation techniques and apply their skills to design and develop data storage solutions to meet a client's requirements.

Unit introduction

Databases underpin many processes in numerous aspects of modern society. From stock control systems for large multi-outlet online retailers to the smallest niche internet forums, databases are a repository of information that make up the world wide web as we know it. Database developers understand and use practical skills utilising technologies that will enable them to design and develop databases that can be used by many different connecting systems.

In this unit, you will examine the structure of data and how an efficient data design follows through into an effective, useful database. You will investigate database management systems (DBMS) and apply practical skills in designing and developing a database within a given DBMS.

This unit will provide you with the knowledge, and skills needed for progression on to higher education programmes in Information Technology.

Learning aims

In this unit you will:

A Understand how the principles of relational database models, data storage and normalisation are used to create effective relational database solutions.

B Design a relational database solution to meet client's requirements.

C Develop a relational database solution to meet client's requirements.

Summary of unit

Learning aim	Key content areas	Assessment approach
A Understand how the principles of relational database models, data storage and normalisation are used to create effective relational database solutions	**A1** Relational database management systems **A2** Manipulating data structures and data in relational databases **A3** Normalisation **A4** Planning a relational database solution in response to a client brief	Conduct research to analyse how the principles of relational database management systems, data storage and normalisation are used to meet a specific purpose and develop planning evidence to meet a client's requirements.
B Design a relational database solution to meet client requirements	**B1** Relational database design techniques and processes **B2** Design documentation **B3** Reviewing and refining designs	Produce, review and refine designs in an iterative process to meet a client's brief.
C Develop a relational database solution to meet client requirements	**C1** Producing a database solution **C2** Testing the database solution **C3** Reviewing the database solution **C4** Optimising the database solution	Use tools and techniques to create a relational database solution to meet a client's requirements.

Content

The essential content is set out under content areas. Students must cover all specified content before the assessment. All topics require students to apply knowledge, analyse and evaluate.

Learning aim A: Understand how the principles of relational database models, data storage and normalisation are used to create effective relational database solutions

A1 Relational database management systems

- Types of relational database management systems (RDBMS) and their operating system support
  - desktop databases
  - server databases, to include:
    - My Structured Query Language (MySQL)
    - Oracle®
- Types of relational data structure concepts
  - relation
  - attribute
  - domain
  - tuple
  - degree
  - cardinality
- Relational algebra sets and symbols
  - union
  - intersect
  - join and select
- Relational keys
  - super key
  - candidate key
  - primary key
  - foreign key
- Integrity constraints
  - entity integrity
  - referential integrity
- Entity relationship types
  - one-to-one
  - one-to-many
  - many-to-many

A2 Manipulating data structures and data in relational databases

Defining, modifying and removing data structures and data

- Updating, inserting, modifying and deletion
- Retrieval of data for:
    o queries
    o reports

A3 Normalisation

The role of normalisation in developing efficient data structures

- Anomalies
    o update
    o insertion
    o deletion
- Keys
    o primary
    o foreign
    o composite
- Referential integrity
- Data dictionary
- Stages of normalisation
    o un-normalised form (UNF)
    o first normal form (1NF)
    o second normal form (2NF)
    o third normal form (3NF)

A4 Preliminary scoping of a relational database solution in response to a client brief

- Purpose, to include:
    o problem to be solved
    o technical requirements
- Research
    o existing databases
    o structuring data, to include:
        – tables
        – keys
    o available resources
- Technical vocabulary
- Logical structure

Learning aim B: Design a relational database solution to meet client requirements [MY-TPR]

B1 Relational database design techniques and processes

Techniques and processes to consider when designing relational databases

- Entity relationship modelling
  - conceptual
    - entity names
    - relationships
    - relationship types
  - logical
    - entity names
    - relationships
    - relationship types
    - attributes
    - primary keys
    - foreign keys
- Relational algebra
  - one to many
  - one to one
  - many to many
  - AND
  - OR
  - NOT
  - $>$
  - $<$
  - $\geq$
  - $\leq$
- DBMS selection, to include:
  - desktop software
  - Cloud/Server-based
- Database implementation techniques
  - prototyping
  - testing
- Quality, effectiveness and appropriateness of the solution
  - correctness of data
  - relationships between data
  - data integrity
  - normalisation

B2 Design documentation

Design specification

- Requirements of the brief

- Audience

- Purpose

- Client requirements

- Legal and ethical considerations
  - data protection legislation
  - applicable regulations

- Data structure designs
  - data dictionaries
    - tables
    - field names
    - field lengths
    - data types
    - validation
  - entity relationship modelling
  - normalisation

- User interface design
  - form design
    - input fields
    - calculated fields
    - disabled fields
    - combo boxes
    - list boxes
    - radio buttons/groups
    - validation
    - masks
    - user help
  - menu design
    - action buttons to initiate tasks
  - queries
    - multiple criteria
    - form values
    - wild cards
    - action queries
    - calculated queries

- o reports
  - – calculated fields
  - – grouping
  - – presentation of data
  - – layouts
  - – conditional formatting
- o task automation, to include:
  - – macros
  - – scripts
  - – program code
- Test plans to check:
  - o data integrity
  - o functionality
  - o accessibility
  - o usability
- Implementation plan
- Timescales

B3 Reviewing and refining designs

- Self-review:
  - o areas for consideration:
    - – suitability for user
    - – meeting client requirements
    - – legal and ethical constraints
    - – consistency
- Refining ideas and solutions
- Updating design specification documentation

Learning aim C: Develop a relational database solution to meet client requirements [MY-TPR]

C1 Producing a database solution

Use of an appropriate database management system and Structured Query Language (SQL) to produce a database solution to meet client's requirements

- Creating, setting up and maintaining data tables
- Creating links/relationships between data tables
- Applying data validation rules

- Generating outputs, to include:
  - user-generated queries
  - automated queries
  - reports
- User interface, to include:
  - navigation
  - data entry forms
  - child forms
- Task automation
- Populating the database
  - importing
  - adding data
  - manipulating data

C2 Testing the database solution Different types of testing
  - referential integrity
  - functionality
- Selection and use of appropriate test data
  - erroneous
  - extreme
  - normal
- Object testing
  - tables
  - queries
  - reports
  - forms
  - menus
- Usability testing
  - selecting suitable test users
  - devising suitable usability tests
- Gathering feedback from users
- Producing appropriate test documentation
- Making use of testing outcomes to improve and/or refine the database solution.

C3 Reviewing the database solution

Criteria for use when reviewing the database solution against

- Quality of the database
- Fitness for purpose
- Suitability against the original requirements

- Legal and ethical constraints
- Strengths and improvements

C4 Optimising the database solution

- Data types
- Data sizes, to include:
  - size on disk
  - data storage requirements e.g. image storage
- Many tables, to include:
  - overheads for many tables
  - query complexity
- Query optimising, to include:
  - select specific columns
  - efficiency of joins/sub-queries.

Assessment criteria

Learning aim A: Understand how the principles of relational database models, data storage and normalisation are used to create effective relational database solutions

Pass	Merit	Distinction
A.P1 Demonstrate an adequate understanding of how the principles of relational database models, data storage and normalisation are used to provide reliable data structures to meet a specific purpose, using partially relevant examples. **A.P2** Carry out adequate research into relational database models, data storage and normalisation to produce a preliminary scoping document that partially meets the client's requirements.	**A.M1** Demonstrate a good understanding of how the principles of relational database models, data storage and normalisation are used to provide reliable data structures to meet a specific purpose, using examples that are mostly relevant and appropriate. **A.M2** Carry out mostly detailed research into relational database models, data storage and normalisation to produce a preliminary scoping document that considers most of the client's requirements.	**A.D1** Carry out effective research to demonstrate a thorough understanding of the principles of relational database models, data storage methods and normalisation and how to comprehensively meet the client's requirements in a preliminary scoping document, using pertinent examples.

Learning aim B: Design a relational database solution to meet client requirements

Pass	Merit	Distinction
B.P3 Produce a design and documentation for a relational database solution to meet some of the client's requirements. **[IS-WC]**	**B.M3** Produce a design and documentation for a relational database solution to meet most of the client's requirements.	**B.D2** Produce a design and documentation for a relational database solution to comprehensively meet the client's requirements.

Learning aim C: Develop a relational database solution to meet client requirements

Pass	Merit	Distinction
C.P4 Use tools, techniques, processes and testing to produce a relational database solution that meets some of the client's requirements. **[SP-C&I]**	**C.M4** Use tools, techniques, processes and testing to produce a relational database solution that meets most of the client's requirements.	**C.D3** Use tools, techniques, processes and testing to produce a relational database solution that comprehensively meets the client's requirements.

Transferable skills

Managing Yourself	Effective Learning	Interpersonal Skills	Solving Problems
MY – TPR *	EL – MOL	IS – WC √	SP – CT
MY – PS&R	EL – CL	IS – V&NC	SP – PS
MY – COP	EL – SRS	IS – T	SP- C&I √
MY – PGS	EL- PRS	IS – C&SI	

Table key

*	Signposted to indicate opportunities for development as part of wider teaching and learning.
√	Embedded in teaching, learning and assessment
Blank	TS not embedded or signposted in unit

Essential information for Pearson Set Assignment Briefs (PSAB)

Pearson sets the assignment for the assessment of this unit.

The PSAB will take 15 hours to complete.

The PSAB will be marked by centres and verified by Pearson.

The PSAB will be valid for the lifetime of this qualification.

Assessing the PSAB

You will make assessment decisions for the PSAB using the assessment criteria provided.

Section 1 gives information on PSABs and there is further information on our website.

Further information for teachers and assessors

Resource requirements

For this unit, students must have access to:

- software resources that will allow them to use tools and techniques (as given in the unit content) to design and develop a relational database.
- a suitable RDBMS, e.g. Access^{TM}, MySQL, Oracle.

Essential information for assessment decisions

Learning aim A

For distinction standard, students will provide a clear and balanced evaluation of relational database principles and a comparison of the advantages each stage of normalisation offers to the effectiveness of the data model. Students will also provide clear examples of normalisation within relational data models. Students will articulate their arguments and views concisely and professionally, and evaluate concepts, ideas and actions in order to reach reasoned and valid conclusions. The scoping document will demonstrate high-quality written communication through the use of accurate and fluent technical vocabulary to support a well-structured and considered response that clearly connects chains of reasoning.

For merit standard, students will undertake an in-depth analysis of relational database principles and normalisation and be able to articulate this using appropriate examples. There will be detailed explanation of normalisation and a clear discussion on how the process improves the efficiency of a relational database. Students will use mostly appropriate diagrams and mostly relevant examples to enable the concept to be relayed effectively. The scoping document will be mostly technically accurate and will demonstrate good-quality written communication.

For pass standard, students will explain the structure of data and how suitable database management systems, with which they are familiar, allow data to be manipulated and presented. Students will show an understanding of normalisation and the process involved; they will also support their explanations with some relevant examples. The scoping document may contain some technical inaccuracies and may not always be clear or fluent.

Learning aim B

For distinction standard, students will make accomplished use of relational database design skills to produce a design solution. The design of data structures and management will demonstrate thorough understanding of the client's requirements and user needs.

A design specification, project timescale and test plan will be created through effective design skills and techniques. The design specification will comprehensively meet the client's requirements.

For merit standard, students will make good use of relational database design skills to produce a design solution. The design of data structures and management will demonstrate good understanding of the client's requirements and user needs.

A design specification, project timescale and test plan will be created through good design skills and techniques. The design specification will meet most of the client's requirements.

For pass standard, students will make basic use of relational database design skills to produce a design solution. The design of data structures and management will demonstrate partial understanding of the client's requirements and user needs.

A design specification, project timescale and test plan will be created through appropriate design skills and techniques. The design specification will partially meet the client's requirements.

Learning aim C

For distinction standard, students will make effective use of tools and techniques to build a relational database solution that comprehensively meets the client's requirements. Effective understanding of data management will be demonstrated through the development of a fully functional relational database.

Students will conduct effective object and usability testing. Students will use the outcomes of the testing and a thorough self-review of their relational database to make considered refinements to the final relational database.

For merit standard, students will make good use of tools and techniques to build a relational database solution that meets most of the client's requirements. Good understanding of data management will be demonstrated through the development of a functional relational database.

Students will conduct appropriate object and usability testing. Students will use the outcomes of the testing and a self-review of their relational database to make appropriate refinements to the final relational database.

For pass standard, students will make basic use of tools and techniques to build a relational database solution that partially meets the client's requirements. Basic understanding of data management will be demonstrated through the development of an adequately functional relational database.

Students will conduct straightforward object and usability testing. Students will use the outcomes of the testing and a self-review of their relational database to refine the final relational database.

5 Planning your programme

Supporting you in planning and implementing your programme

There will be lots of free teaching and learning support to help you deliver the new qualifications, including:

- Our Planning and Teaching Guide will help you to plan how to deliver the content and assessments that make up Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate) qualification. It also highlights opportunities to develop the transferable skills identified within the units in this specification.

- Sample Assessment materials are available for each external unit to help you to plan and prepare for assessments.

- Our mapping document highlights key differences between the new qualification and Pearson BTEC Level 3 National Extended Certificate in Information Technology 601/7575/8, which this qualification replaces.

Is there a student entry requirement?

As a centre it is your responsibility to ensure that students who are recruited have a reasonable expectation of success on the programme. There are no formal entry requirements but we expect students to have qualifications at or equivalent to Level 2.

Students are most likely to succeed if they have:

- five GCSEs at good grades, and/or
- BTEC qualification(s) at Level 2
- achievement in English and mathematics through GCSE or Functional Skills.

Students may demonstrate ability to succeed in various ways. For example, students may have relevant work experience or specific aptitude shown through diagnostic tests or non-educational experience.

6 Understanding the qualification grade

Awarding and reporting for the qualification

This section explains the rules that we apply in awarding a qualification and in providing an overall qualification grade for each student. It shows how all the qualifications in this sector are graded.

The awarding and certification of these qualifications will comply with regulatory requirements.

Eligibility for an award

In order to be awarded a qualification, a student must:

- complete and **have an outcome** (D, M, P, N or U) for all units within a valid combination
- achieve the **minimum number of points** at a grade threshold.

Awarding the qualification grade

The final grade awarded for a qualification represents an aggregation of a student's performance across the qualification. As the qualification grade is an aggregate of the total performance, there is some element of compensation in that a higher performance in some units may be balanced by a lower outcome in others.

BTEC Nationals are Level 3 qualifications and are awarded at the grade ranges shown in the table below.

Qualification	Available grade range
Extended Certificate	P to D*

The *Awarding the qualification grade* table, shown further on in this section, shows the minimum thresholds for calculating these grades. The table will be kept under review over the lifetime of the qualification. The most up-to-date table will be issued on our website.

Pearson will monitor the qualification standard and reserves the right to make appropriate adjustments.

Students who do not meet the minimum requirements for a qualification grade to be awarded will be recorded as Unclassified (U) and will not be certificated. They may receive a Notification of Performance for individual units. The *Information Manual* gives full information.

Points available for internal units

The table below shows the number of **points** available for internal units. For each internal unit, points are allocated depending on the grade awarded.

Grade	Unit size (60 GLH)
U	0
Pass	6
Merit	10
Distinction	16

Points available for external units

Raw marks from the external units will be awarded **points** based on performance in the assessment. The table below shows the **minimum number of points** available for each grade in the external units.

Grade	Unit size (120 GLH)
U	0
Near Pass	8
Pass	12
Merit	20
Distinction	32

Pearson will automatically calculate the points for each external unit once the external assessment has been marked and grade boundaries have been set. For more details about how we set grade boundaries in the external assessment please go to our website.

Claiming the qualification grade

Subject to eligibility, Pearson will automatically calculate the qualification grade for your students when the internal unit grades are submitted and the qualification claim is made. Students will be awarded qualification grades for achieving the sufficient number of points (with valid combinations) within the ranges shown in the relevant *Awarding the qualification grade* table for the cohort.

Awarding the qualification grade

Applicable for registration from 1 August 2025.

Extended Certificate (360 GLH)

Grade	Points threshold
U	0
Pass	36
Merit	52
Distinction	74
Distinction *	90

The table is subject to review over the lifetime of the qualification. The most up-to-date version will be issued on our website.

Example grading table for Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate)

Unit number	GLH	Type (Int/Ext)	Grade	Unit points
1	120	Ext	Merit	24
2	120	Ext	Near Pass	8
3	60	Int	Pass	6
4	60	Int	Merit	10
TOTAL	**360**		**Pass**	**48**

Appendix 1 Glossary of terms used for internally assessed units

Term	Definition
Adequate	Student work is satisfactory or acceptable in quality and quantity.
Analyse	Students break the issue/situation down into the key elements and show their understanding of the issues/situation applied to the scenario/context. Responses would be significantly beyond generic.
Apply/use/employ	Students implement a method, technique, process or approach in an activity.
Assess	Students give careful consideration to all the factors or events that apply, identify which are the most important or relevant and make a judgement on the importance of the factors.
Carry out	Students demonstrate skills through practical activities, in line with certain requirements.
Clear/ly	The qualities required are well demonstrated, unambiguous and beyond a basic level.
Coherent	Student intentions are clear, logically structured and can be interpreted by others.
Compare	Students show knowledge and understanding by identifying the main factors relating to two or more items/situations or aspects of a subject that is extended with the required explanations, e.g. similarities/differences, advantages/disadvantages, impacts.
Comprehensive	Used to describe either scope or depth, e.g. • Student work is well developed and thorough covering all aspects/information in terms of both depth and breadth Or: • Students demonstrate in-depth and accurate understanding of the aspects being assessed.
Confident	Student work demonstrates well-developed and secure application of skills or processes that are significantly beyond a basic level.
Consistent	Students demonstrate reliable and constant practice that maintains a set standard.
Create/produce	Students generate an idea/outcome to specific criteria.
Demonstrate	Students carry out and apply knowledge, understanding and/or skills in a practical situation.
Describe	Students provide an account of something, or highlight a number of key features of a given topic or process that shows a level of understanding.
Detailed	Students cover most if not all of the expected requirements and demonstrate a high level of understanding.

Term	Definition
Develop	Students apply a process of improving/progressing skills, concepts or work in order to produce outcomes.
Discuss	An issue, situation, process will be presented and the student will need to break the issue/situation/process down into the key elements, show their understanding of the issues/situation/process applied to the scenario/context (so generic answers are not acceptable), and show interrelationship in their answers.
Effective	Students demonstrate skills or provide outcomes that are well developed with a range of proficient qualities and that achieve objectives
Evaluate	Students consider various aspects of a subject's qualities in relation to its context such as: strengths or weaknesses, advantages or disadvantages, pros or cons. They will come to a judgement supported by evidence which will often be in the form of a conclusion.
Examine	Students demonstrate an ability to thoroughly inspect something in order to determine its qualities beyond a basic exploration.
Explain	Students can give an insight into the topic showing some level of understanding by providing reasons or examples.
Explore	Students undertake practical research or investigation to develop their skills or understanding of the topic/activity.
Implement	Students take actions or measures to put something into effect.
Investigate	Students perform a systematic inquiry into a topic using research skills, usually to demonstrate their understanding of a topic.
Justify	Students give relevant and logical reasons or evidence to support their actions or opinions.
Partial/some	To an extent, but not completely. Students do not include all of the requirements.
Perform	Students demonstrate a range of skills required to complete a given activity.
Prepare	Students organise a task/equipment/individuals/activities in advance of carrying it out.
Realistic/feasible	Students demonstrate insight into the logistics and manageability of proposals/plans/objectives/ideas and show consideration of the potential to achieve the outcomes.
Refine/optimise	Students make considered improvements to outcomes.
Review	Students consider evidence in order to make judgements about the qualities.
Understand	Students demonstrate insight or ability to interpret a subject.
Undertake	Students demonstrate skills through practical activities, often referring to given processes or techniques.

Appendix 2 Transferable Skills framework

Code = transferable skill initials-skill cluster initials

Managing yourself

Code	Skill cluster	Performance Descriptor
MY-TPR	Taking personal responsibility	• Demonstrates understanding of their role and responsibilities and the expected standards of behaviour. • Demonstrates compliance with codes of conduct and ways of working. • Makes use of available resources to complete tasks. • Manages their time to meet deadlines and the required standards. • Demonstrates accountability for their decisions or actions.
MY-PS&R	Personal strengths and resilience	• Identifies own personal strengths and demonstrates the ability to use these in relevant areas. • Demonstrates the ability to adapt own mindset and actions to changing situations or factors. • Uses challenges as learning opportunities.

Code	Skill cluster	Performance Descriptor
MY-COP	Career orientation planning	• Undertakes research to understand the types of roles in the sector in which they could work. • Reviews own career plans against personal strengths and identifies areas for development to support progression into selected careers. • Takes part in sector-related experiences to support career planning.
MY-PGS	Personal goal setting	• Sets SMART goals using relevant evidence and information. • Reviews progress against goals and identifies realistic areas for improvement. • Seeks feedback from others to improve own performance.

Effective learning

Code	Skill cluster	Performance Descriptor
EL-MOL	Managing own learning	• Maintains a focus on own learning objectives when completing a task. • Demonstrates the ability to work independently to complete tasks. • Reviews and applies learning from successful and unsuccessful outcomes to be effective in subsequent tasks.
EL-CL	Continuous learning	• Engages with others to obtain feedback about own learning progress. • Responds positively to feedback on learning progress from others. • Monitors own learning and performance over the short and medium term.
EL-SRS	Secondary research skills	• Defines the research topic or question. • Uses valid and reliable sources to collate secondary data. • Interprets secondary data and draws valid conclusions. • Produces a reference list and cites sources appropriately.
EL-PRS	Primary research skills	• Defines the research topic or question. • Carries out primary data collection using appropriate and ethical research methodology. • Interprets primary data to draw valid conclusions

Interpersonal skills

Code	Skill cluster	Performance Descriptor
IS-WC	Written communication	• Produces clear formal written communication using appropriate language and tone to suit purpose.
IS-V&NC	Verbal and non-verbal communications	• Uses verbal communication skills confidently to suit audience and purpose. • Uses body language and non-verbal cues effectively. • Uses active listening skills and checks understanding when interacting with others.
IS-T	Teamwork	• Engages positively with team members to understand shared goals and own roles and responsibilities. • Respectfully considers the views of team members and consistently shows courtesy and fairness. • Completes activities in line with agreed role and responsibilities. • Provides support to team members to achieve shared goals.
IS-C&SI	Cultural and social intelligence	• Demonstrates awareness of own cultural and social biases. • Demonstrates diversity, tolerance and inclusivity values in their approach to working with others.

Solving problems

Code	Skill cluster	Performance Descriptor
SP-CT	Critical thinking	• Demonstrates understanding of the problem or issue to be addressed. • Makes use of relevant information to build ideas and arguments. • Assesses the importance, relevance and/or credibility of information and ideas. • Analyses, interprets and evaluates information to present reasoned conclusions.
SP-PS	Problem solving	• Presents a clear definition of the problem. • Gathers relevant information to formulate proposed solutions. • Selects relevant and significant information to formulate proposed solutions. • Identifies negative and positive implications of proposed solutions. • Presents and justifies selected solutions to problems.
SP-C&I	Creativity and innovation	• Identifies new and relevant ideas to help solve a problem. • Refines ideas into workable solutions based on test results and/or feedback.

Appendix 3 Digital Skills framework

Problem solving

Using digital tools to analyse and solve problems:

Performance descriptor	Unit mapping
Use digital tools and techniques for research, collaboration and resolution of problems.	Unit 3, content area A and Unit 4 content area A
Have up-to-date knowledge of ways that technology is used within a sector.	Unit 3, content area A and Unit 4 content area A
Present ideas and finding using digital tools.	Unit 3, content area B and Unit 4 content area B
Use digital tools to manipulate data.	Unit 4 content area C

Digital collaboration and communication

Using digital tools to communicate and share information with stakeholders:

Performance descriptor	Unit mapping
Understand and use digital collaboration and communication platforms.	N/A
Use collaboration tools to meet with, share and collaborate with customers and colleagues.	N/A

Transacting digitally

Using digital tools to set up accounts and pay for goods/services:

Performance descriptor	Unit mapping
Use online systems to access and update digital records.	N/A
Set-up accounts to complete transactions.	Unit 3, content area C

Digital security

Identify threats and keep digital tools safe:

Performance descriptor	Unit mapping
Understand the types of malware.	Unit 1, content area B and Unit 2 content area A
Understand the threats involved in carrying out online activities.	Unit 2, content area A
Protect personal and organisation information and data.	Unit 2, content area A and B
Keeping systems secure.	Unit 2, content area A and B

Handling data safely and securely

Follow correct procedures when handling personal and organisational data:

Performance descriptor	Unit mapping
Manage passwords and keep them secure.	Unit 1, content area B
Identify website and services that are secure and insecure.	Unit 1, content area B
Understand the digital policy for a sector.	Unit 3, content area A and Unit 4 content area A
Understand the impact of online data.	Unit 1, content area C
Understand copyright and intellectual property.	Unit 3, content area A

Appendix 4 Sustainability framework

Sustainable development goal	Unit mapping
SDG 1: No poverty	N/A
SDG 2: Zero hunger	N/A
SDG 3: Good health and wellbeing	N/A
SDG 4: Quality education	N/A
SDG 5: Gender equality	N/A
SDG 6: Clean water and sanitation	N/A
SDG 7: Affordable and clean energy	N/A
SDG 8: Decent work and economic growth	N/A
SDG 9: Industry, innovation and infrastructure	Unit 1, content area A and Unit 2, content area A
SDG 10: Reduced inequalities	Unit 1, content area F and Unit 3, content area C
SDG 11: Sustainable cities and communities	N/A
SDG 12: Responsible consumption and production	Unit 1, content area F
SDG 13: Climate action	N/A
SDG 14: Life below water	N/A
SDG15: Life on land	N/A
SDG 16: Peace, justice and strong institutions	Unit 1, content area F and Unit 3, content area B
SDG 17: Partnerships for the goals	N/A

Pearson

BTEC