Pearson Level 3 V Level in Digital Systems and Data

Specification

First teaching September 2027
Final Draft V1

Pre-Accreditation Draft

This draft qualification has not yet been accredited by Ofqual. It is published to enable teachers to have early sight of our proposed approach to the Pearson Level 3 V Level in Digital Systems and Data. Further changes may be required and no assurance can be given at this time that the proposed qualification will be made available in its current form.

About Pearson

At Pearson, our purpose is simple: to help people realise the life they imagine through learning. We believe that every learning opportunity is a chance for a personal breakthrough. That's why our c.18,000 Pearson employees are committed to creating vibrant and enriching learning experiences designed for real-life impact. We are the world's lifelong learning company, serving customers in nearly 200 countries with digital learning and assessments experiences, verified skills, and credentials. For us, learning isn't just what we do. It's who we are.

Visit us at plc.pearson.com.

Pre-Accreditation Draft

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

All information in this specification is correct at time of publication

Publication code VQ000576
All the material in this publication is copyright
© Pearson Education Limited 2026

Introduction

About V Levels

V Levels are Level 3 vocational qualifications developed for post-16 students who want to explore a sector, or multiple sectors, without specialising too early. Available in a single size of 360 guided learning hours (GLH), they give students the flexibility to build a broader programme of study that reflects their interests and future ambitions.

Students can combine a V Level with other V Levels, other vocational qualifications, A levels or, where appropriate, English and maths qualifications. This flexibility helps them to keep their options open while developing valuable knowledge and skills.

Based on the Department for Education (DfE) subject content, V Levels combine theory, practical learning and transferable skills. Through applied work-related learning, students develop understanding of a sector and build the confidence to take their next step into higher education, apprenticeships or further technical study.

Unlike T Levels, V Levels provide a broad vocational pathway rather than preparing students for a specific occupational role. They help students explore opportunities, understand progression routes and make informed decisions about their future.

Why choose V Levels from Pearson?

Drawing on decades of vocational expertise and our strong partnerships with educators, employers and higher education institutions, Pearson has developed V Levels that support meaningful progression while giving educators the tools and support they need to deliver with confidence.

Authentic vocational learning. Our qualifications are built around practical learning and real-world application. Students can connect what they learn in the classroom with how the sector operates in practice, helping them to stay engaged, deepen their understanding and apply their learning in different contexts.

Assessments you can trust. Our assessments are vocationally relevant, straightforward to deliver and designed so that the full range of students can demonstrate what they know and can do. This gives you confidence in student outcomes.

Pathways and progression routes. Our broad range of academic and vocational qualifications helps you to build coherent study programmes that reflect students' aspirations and support progression to positive destinations.

Confident delivery. You can deliver our V Levels with confidence through our comprehensive teaching and learning support resources, professional development offer and dedicated support from our Subject Advisors.

This specification document should be used in conjunction with the *Pearson V Levels Supplementary Specification*, available on our website.

Pre-Accreditation Draft

Contents

1 Pearson Level 3 V Level in Digital Systems and Data – Purpose 1

Who is the qualification for 1

How will students apply their learning? 1

What knowledge and understanding will students develop? 1

Sector-specific skills 2

Transferable skills 2

Which other qualifications can be taken alongside this V Level? 2

What can the qualification lead to? 2

2 Qualification overview and key information 4

Qualification at a glance 4

Total qualification time 6

Qualification structure 7

Assessment 8

Assessment objectives 8

Breakdown of assessment objectives (AOs) 8

Non-exam assessment (NEA) 9

Examined assessment 10

Synoptic assessment 10

Language of assessment 10

Grading of the qualification 11

UCAS tariff points 11

3 Units 12

Understanding your units 12

Non-exam assessment (NEA) 13

Examined assessment units 15

Unit 1: Presenting Data Effectively 17

Unit 2: Securing Digital Systems 41

Unit 3: Configuring Digital Systems 62

Unit 4: Creating Digital Solutions 82

Unit 5: Understanding Digital Systems 103

4 Planning your programme 131

Is there a student entry requirement? 131

Pre-Accreditation Draft

What level of sector knowledge is needed to teach this qualification? 131
What resources are required to deliver this qualification? 131
What makes good vocational teaching? 131
5 Final grading and awarding 132
Awarding and reporting for the qualification 132
Eligibility for an award 132
Calculation of the qualification grade 133
The minimum uniform marks required for each grade for each unit 133
Results issue 133
6 Resources and support 134
Support for setting up your course and preparing to teach 134
Delivery Guide 134
Support for teaching and learning 134
Support for assessment 134
Centre standardisation materials for NEA units 134
Training and support from Pearson 135
Appendix 1 136
Glossary of terms used for NEA marking grids 136
Appendix 2 141
Command word taxonomy for examined assessment 141
Appendix 3 142
Mapping between Department for Education (DfE) subject content and Pearson content and Pearson Level 3 V Level in Digital Systems and Data 142

Pre-Accreditation Draft

1 Pearson Level 3 V Level in Digital Systems and Data – Purpose

Who is the qualification for

The Pearson Level 3 V Level in Digital Systems and Data is for post-16 students who want to explore their options through applied learning. It is suitable for students who are interested in careers in Digital and Technologies and want to develop industry-relevant knowledge, understanding and skills alongside other Level 3 qualifications in their study programme, to progress to related higher education courses or apprenticeships.

The qualification develops students' understanding of how digital systems, data and technologies are used to meet user and organisational needs. Students will understand how digital systems function, how data and information are used to support decision making, and how digital technologies can be applied to solve problems and develop solutions. The qualification focuses on the applied use of digital concepts and principles in defined organisational contexts, enabling students to develop the knowledge and understanding needed to work effectively with digital systems, data and solutions.

How will students apply their learning?

The students will apply their knowledge, understanding and skills to:

- prepare, analyse, interpret and present data from different sources to support conclusions and decision making
- apply security protocols and interpret system information to detect and escalate cyber security concerns
- prepare, configure and assure readiness of digital systems to meet user needs (optional) **or**
- design and create a digital solution to meet defined user needs (optional).

What knowledge and understanding will students develop?

Students will develop knowledge and understanding of:

- **Digital systems creation, configuration and fault finding:** the components and operation of digital systems; configuration, access, connectivity, storage and security settings; testing, performance, readiness and system dependencies.
- **Digital systems security:** the threats, issues, protocols and technologies associated with digital systems; preventative and protective actions; authentication requirements and access controls

Pre-Accreditation Draft

- **Responsible practice, communication and ways of working with digital systems:** intellectual property, ownership, attribution, responsible practice, sustainability, prompts and structured inputs, bias, limitations, transparency and human oversight.
- **Principles of problem solving, programming logic and digital solution design:** requirements, constraints, abstraction, decomposition, sequencing, selection, iteration, programming logic, testing, refinement and justification of design decisions.

Sector-specific skills

Students will develop and have opportunity to practise the following sector-specific skills:

- data analysis
- systems configuration
- security monitoring
- system testing (optional) **or**
- solution design (optional).

Transferable skills

Students are expected to develop the following transferable skills:
analysing and critical thinking

- investigating
- decision making
- planning
- problem solving
- communicating
- collaboration.

The Department for Education's *Framework for transferable skills and work-related behaviours* sets out the common language used for transferable skills and work-related behaviours.

Which other qualifications can be taken alongside this V Level?

This V Level can be taken alongside other complementary Level 3 qualifications such as V Levels, A Levels and, where appropriate, English and maths qualifications.

What can the qualification lead to?

This qualification, when taken as a part of a coherent study programme, can lead to progression to the following:

- BSc (Hons) Computer Science – potential career outcomes include data scientist, systems engineer or AI data specialist

Pre-Accreditation Draft

- BSc (Hons) Digital Forensics – potential career outcomes include cyber security specialist, network engineer and cyber risk analyst
- BSc (Hons) Software Engineering – potential career outcomes include software engineer, machine learning engineer and UX engineer

Pre-Accreditation Draft

2 Qualification overview and key information

Qualification at a glance

Qualification title	Pearson Level 3 V Level in Digital Systems and Data
Qualification Number (QN)	XXX/XXX/X
Regulation start date	XX/XX/XXXX
Operational start date	01/08/2027
First certification date	Summer 2029
Approved age ranges	16–18 18+ 19+
Total qualification time (TQT)	475
Guided learning hours (GLH)	360
Duration	Intended to be taken over a 2 year programme of study.
Entry requirements	Students do not need any prior knowledge, skills or qualifications to take this qualification.
Qualification requirements	Students must complete a total of 4 units: • 3 mandatory units • 1 optional unit.
Assessment model	Units 1, 2, 3 and 4 are assessed by Non-exam Assessment (NEA). These are marked by centres but set and moderated by Pearson. Unit 5 is assessed by examined assessment, which is set and marked by Pearson. This assessment is terminal, meaning it must be taken in the students' final assessment series for the qualification. Further information on assessment requirements is provided in each unit.
Examined assessment availability	Assessments are available in May/June each academic year. First assessment: May/June 2029

Pre-Accreditation Draft

Qualification title	Pearson Level 3 V Level in Digital Systems and Data
NEA submission	There is one submission window in May each academic year . Students must be registered for the qualification and entered for the unit before you can submit NEA outcomes for moderation.
Resubmission of NEA	Students have one resubmission opportunity for each NEA. One internal resubmission opportunity may be approved by the centre before marks and evidence are submitted for moderation. Information on the conditions for authorising NEA resubmissions is in the *Pearson V Levels Supplementary Specification.*
Retakes	NEA - following moderation, students can retake an NEA in the next available assessment window. Unless specified, students must respond to the NEA released for the series they are taking the retake. Examined assessment - students may retake the assessment in any available series, subject to the terminal assessment rule.
Grade aggregation	Grade aggregation is compensatory. This means that there are no must-pass units. Students accumulate marks across individual tasks and units, so stronger performance in one area or unit can balance less secure performance elsewhere when the overall qualification result is calculated.
Grading	The qualification and units are graded as A*-E plus P (Pass) and U (Unclassified).
UCAS points	This qualification is recognised in the UCAS tariff tables. You will find more information on the UCAS website.

Pre-Accreditation Draft

Total qualification time

For all regulated qualifications, Pearson specifies a Total Qualification Time (TQT). This is the total number of hours that it is estimated students will need to complete and show achievement for the qualification. Within the TQT, Pearson specifies the number of Guided Learning Hours (GLH). These are the hours that we estimate a centre delivering the qualification will provide.

Guided learning means activities such as lessons, tutorials, online instruction, supervised study, and feedback on performance where teachers or assessors are directly involved in teaching, supervising or invigilating students. It also includes the time students spend taking examined assessments under supervised conditions.

In addition to guided learning, students will spend time on other activities directed by teachers or assessors. These may include private study, assessment preparation and unsupervised assessment activities, such as preparatory reading, revision and independent research.

The Pearson Level 3 V Level in Digital Systems and Data has:

Total Qualification Time: 475 hours

Guided Learning Hours: 360 hours.

Centres should take these hours into account when planning their programme. However, they should also use their professional judgement to determine the amount of guided learning and study time across the units

Pre-Accreditation Draft

Qualification structure

This table shows all units and the weighting they contribute to the qualification. Students must complete 3 mandatory units and 1 optional unit.

Unit number	Unit title	GLH	Weighting	How assessed	Mandatory or optional
1	Presenting Data Effectively	72 GLH	20%	Centre marked, Pearson moderated NEA	Mandatory
2	Securing Digital Systems	72 GLH	20%	Centre marked, Pearson moderated NEA	Mandatory
3	Configuring Digital Systems	72 GLH	20%	Centre marked, Pearson moderated NEA	Optional
4	Creating Digital Solutions	72 GLH	20%	Centre marked, Pearson moderated NEA	Optional
5	Understanding Digital Systems	144 GLH	40%	Examination, Pearson marked	Mandatory (Terminal)

Pre-Accreditation Draft

Assessment

Assessment is designed to meet the purposes of the V Level qualification. It includes a combination of assessment types and different forms or styles that reflect the qualification content. The two types of assessment are: examined assessment and non-exam assessment (NEA). Students will also respond to synoptic assessments within each type.

Assessment objectives

Assessment objectives are the hierarchy of the specific skills and abilities students are expected to demonstrate in all assessments. The assessment objectives, and their weightings, for this qualification are shown below.

Assessment objectives (what students must do)		% in qualification
AO1	Demonstrate knowledge and understanding of concepts, principles, requirements and contextual factors relevant to the subject area	30%
AO2	Apply knowledge and understanding to plan, carry out tasks, produce outputs, and use information appropriately	44.5%
AO3	Analyse and evaluate information, situations and evidence to make judgements, draw conclusions and make recommendations	25.5%

Breakdown of assessment objectives (AOs)

Unit	AO1	AO2	AO3	Total % for assessment objectives
Unit 1: Presenting Data Effectively	10%	55%	35%	20%
Unit 2: Securing Digital Systems	10%	55%	35%	20%
Unit 3: Configuring Digital Systems **OR** Unit 4: Creating Digital Solutions	10%	60%	30%	20%
Unit 5: Understanding Digital Systems	60%	26.4%	13.6%	40%

***Students only do one of either Unit 3 or 4 as these are optional units.

Pre-accreditation Draft

Non-exam assessment (NEA)

Units 1, 2, 3 and are assessed through non-exam assessment (NEA) set by Pearson, marked by centres and moderated by Pearson. NEAs give students the opportunity to apply their knowledge and understanding through realistic work-related tasks and activities. This helps students connect what they know with how it is applied in practice.

For each unit, new NEAs are released once a year through the secure area of our website. Each assessment will be clearly marked with the assessment series and academic year in which it was released. Centres must ensure that they are using the correct assessment for the series in which students have been entered.

Centres will mark the completed assessments using the descriptors in the marking grids provided in each unit.

Unit	NEA description	Window for assessment
Unit 1: Presenting Data Effectively	5 tasks, marked out of a total of 60 marks and completed over 15 hours.	Released in September for May submission. First submission May 2028
Unit 2: Securing Digital Systems	5 tasks, marked out of a total of 60 marks and completed over 15 hours.	Released in September for May submission. First assessment May 2028
Unit 3: Configuring Digital Systems	5 tasks, marked out of a total of 60 marks and completed over 15 hours.	Released in September for May submission. First submission May 2028
Unit 4: Creating Digital Solutions	5 tasks, marked out of a total of 60 marks and completed over 15 hours.	Released in September for May submission. First submission May 2028

Further information about the design and delivery of NEAs, including levels of control, marking, resubmissions and retakes is provided in the *Pearson V Levels Supplementary Specification,* available on our website.

Pre-Accreditation Draft

Examined assessment

Unit 5 Understanding Digital Systems is assessed through an examined assessment that is timetabled, set and marked by Pearson.

The examined assessment takes the form of a written examination taken under supervised conditions, which is then marked and a grade awarded by Pearson.

The examined assessment comprises 40% of the total GLH of the qualification and is weighted accordingly in the calculation of the overall qualification grade.

Unit	Description of external assessment	Assessment
Unit 5: Understanding Digital Systems	A written examination, which is set and marked by Pearson and completed under supervised conditions. It must be taken in the students' final assessment series for the qualification to meet the terminal assessment rule. The examination is worth 110 marks and lasts for 2 hours and 30 minutes.	May/June First assessment May/June 2029

Further information about examined assessments is provided in the *Pearson V Levels Supplementary Specification,* available on our website.

Synoptic assessment

Synoptic assessment requires students to demonstrate that they can apply their overall knowledge, understanding and skills, from across the course of study.

All assessments provide opportunities for students to:

(a) demonstrate the ability to draw together different areas of knowledge, understanding and/or skills from across the full course of study, and

(b) construct and develop an extended line of reasoning which is relevant, coherent and effectively structured.

Synoptic links between teaching content are identified within each unit .

Language of assessment

Assessments for all units will be available in English. All student work must be in English. A student taking the qualification may be assessed in British Sign Language where this is permitted for reasonable adjustment. Further information about reasonable adjustments is provided in the *Pearson V Levels Supplementary Specification,* available on our website.

Pre-Accreditation Draft

Grading of the qualification

The qualification is graded using a scale of A* to E, P (Pass) and U (Unclassified). The overall grade is based on performance across all units. Further information about grading is provided in *Section 5: Final grading and awarding*.

UCAS tariff points

This V Level qualification attract UCAS points. Please go to the UCAS website for full details of the points allocated.

Pre-Accreditation Draft

3 Units

Understanding your units

The units in this specification set out details of all the knowledge and skills a student must acquire, and the assessment requirements that will support you in preparing your students. We have sequenced the units in the order we believe best supports sustained learning, and we recommend that centres deliver them in this order. Where synoptic assessment requires that a unit must be delivered towards the end of the course, this will be stated in the unit guidance.

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

Non-exam assessment (NEA)

Examined assessment.

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

Pre-Accreditation Draft

Non-exam assessment (NEA)

Section	Explanation
Assessment type	This confirms how the unit is assessed, (non-exam assessment (NEA) or examined assessment).
Unit type	This confirms whether the unit is mandatory or optional.
Guided learning hours	This indicates the number of hours of teaching, directed activity and supervised assessment expected.
Unit introduction	This is designed with students in mind. It indicates why the unit is important and how learning is structured.
Teaching content	This details the knowledge and skills that must be taught. It also includes additional information, such as synoptic links, where needed. The content has been purposefully structured to support teaching, learning and assessment, and is presented in a sequence that reflects a logical teaching order while helping students build the knowledge and skills needed for successful assessment. Content outcome statements provide the overarching focus for each area of content, enabling teachers to understand the key themes and intended learning at a glance. The content detail then provides further detail on the breadth and depth of content to be taught, ensuring clarity and consistency in the interpretation and delivery of the specification. All content is mandatory. The content sets out the full requirement for teaching and assessment, except where: • The content statement is followed by 'e.g.' – in these instances, the content is indicative within the topic and is not an exhaustive list of what should or could be covered. This content is included to provide clarity around the interpretation of the topic area by providing indicative areas that might be covered. • content statements include inexhaustive lists, denoted as 'including'. Content following 'including' statements show content that must be taught, but centres may wish to include further examples. Centres should ensure that delivery of content is kept up to date.

Pre-Accreditation Draft

Transferable skills	This dentifies the transferable skills students are expected to develop in the unit and how they will apply them in work-related contexts relevant to the sector.
Assessment summary	This gives a description of the NEA for the unit, including the nature of the tasks, duration and availability.
Marking the NEA	This gives an overview of the approach for marking the NEA.
Marking grid	The marking grid details the descriptors across the mark bands that the teachers/assessors will use to determine the marks to be awarded to students' assessment evidence.
Resource requirements	This section lists any specific resources that you need to be able to teach and for students to take the assessment. For information on support resources see *Section 6: Resources and support*.

Pre-Accreditation Draft

Examined assessment units

Section	Explanation
Assessment type	This confirms how the unit is assessed (non-examined or examined assessment)
Unit type	This confirms whether the unit is mandatory or optional.
Guided learning hours	This indicates the number of hours of teaching, directed activity and supervised assessment expected. It also shows the weighting of the unit in the final qualification grade.
Unit introduction	This is designed with students in mind. It indicates why the unit is important and how learning is structured. It might be applied when progressing to further study.
Teaching content	This gives the content that must be taught for the examined assessment. It also includes additional information, such as synoptic links, where needed. The content has been purposefully structured to support teaching, learning and assessment, and is presented in a sequence that reflects a logical teaching order while helping students build the knowledge and skills needed for successful assessment. Content outcome statements provide the overarching focus for each area of content, enabling teachers to understand the key themes and intended learning at a glance. The content detail then provides further detail on the breadth and depth of content to be taught, ensuring clarity and consistency in the interpretation and delivery of the specification. All content is mandatory. Content will be sampled through the examined assessment over time.
Transferable skills	This identifies the transferable skills students are expected to develop in the unit and how they will apply them in work-related contexts relevant to the sector.
Assessment summary	This sets out the form of examined assessment and the way in which it is used to assess achievement.

Pre-Accreditation Draft

Resource requirements	This section lists any specific resources that you need to be able to teach and for students to take the assessment. For information on support resources see *Section 6: Resources and support*.

Pre-Accreditation Draft

Unit 1: Presenting Data Effectively

Assessment type: **Non-exam assessment (NEA)**

Unit type: Mandatory

Guided learning hours: 72

Introduction

In this unit you will develop knowledge and understanding of how data can be collected, prepared, analysed, and presented to support decision-making in the workplace, and you will examine the importance of data quality, reliability and transparency.

You will explore how organisations use data to identify patterns, trends and relationships to solve problems. You will develop practical skills in preparing datasets by checking data quality and select appropriate methods to interpret results to produce meaningful insights.

You will communicate findings to different audiences, considering suitable presentation formats that include tables, charts, graphs, and written reports to communicate information clearly, accurately and appropriately for a particular purpose.

Students should be given opportunities to develop their knowledge and skills in a range of contexts including different datasets, software and work-related scenarios.

Pre-Accreditation Draft

Pre-Accreditation Draft

Pre-Accreditation Draft

Teaching content

Content area A: Data foundations, structure, preparation, quality, privacy and governance

Content outcome	Content detail
A1 Demonstrate knowledge and understanding of the purpose of data processing	**A1.1 Data and datasets** **A1.1.1** quantitative and qualitative; structured and unstructured; primary and secondary; internal and external data **A1.1.2** records, fields, values and identifiers, including relevant, missing, inaccurate and sensitive fields **A1.1.3** text/string, numeric, date/time and Boolean data types; common data formats and units **A1.1.4** purpose, audience, complexity, accuracy, time and resources as factors affecting level of detail **A1.1.5** preparing, analysing, interpreting and presenting data **A1.1.6** generating insights to support conclusions and decision making in workplace contexts
A2 Demonstrate knowledge and understanding of how data is structured, formatted and defined within datasets from different sources	**A2.1 Data structure, format and definition** **A2.1.1** field definitions, categories, codes, metadata and data dictionaries methodologies, preparation records, analytical methods, assumptions, strengths and limitations across different sources **A2.1.2** source, author, creation date, ownership, version, processing history, field definitions and audit trail **A2.2 Metadata and documentation** **A2.2.1** using documentation to support consistency, reproducibility, interpretation, quality checking and accountability **A2.2.2** levels of detail, aggregation and granularity as factors affecting interpretation, comparability and use

Pre-Accreditation Draft

Content outcome	Content detail
A3 Apply knowledge and understanding of policies and procedures relating to data safety, protection and governance	**A3.1 Data Safety, Privacy and Confidentiality** **A3.1.1** collection purpose and lawful use, data minimisation, accuracy, required consent, retention and secure deletion, Data privacy, Data confidentiality, Responsible data use . **A3.1.2** access controls, permissions, authentication, encryption, secure storage and transfer, breach handling and staff responsibilities **A3.1.3** removing or protecting direct and indirect identifiers; review anonymisation and limit access to authorised users **A3.1.4** lawful and appropriate use of data, protection of personal and sensitive information, transparency and explainability of automated outputs, accountability and human oversight, check accuracy, completeness, relevance, bias and fairness before and during analysis **A3.1.5** recording: data, tools, models, changes, outputs, decisions, responsibilities and retention, correct documentation of analysis
A4 Demonstrate understanding of the requirements, limitations and advantages of using automated and AI-enabled analysis.	**A4.1 Requirements** **A4.1.1** need for human oversight, output explanation, protecting individual rights and maintaining an audit trail **A4.1.2** mitigation of bias in analytical processes **A4.1.3** need to interpret outputs critically, **A4.1.4** explanation of assumptions, limitations and confidence **A4.1.5** establishing quality of underlying data and analysis **A4.1.6** distinction between system-generated findings and human review, interpretation and judgement **A4.1.7** documentation, traceability, explainability, challenge and audit of methods and decisions **A4.1.8** importance of transparency when presenting insights generated and supported by automated and AI-enabled systems

Pre-Accreditation Draft

Content outcome	Content detail
	A4.2 Limitations **A4.2.1** potential sources of bias in: data collection, preparation, processing, drawing conclusions **A4.2.2** reduced accountability, limited challenge, weak auditability and loss of stakeholder trust **A4.2.3** incorrect interpretation of analysed outputs **A4.2.5** assumptions, treatment of missing values, limitations, uncertainty and confidence **A4.2.6** consequences of unexplained automated outputs **A4.2.7** misinterpretation of outputs and conclusions **A4.2.8** unjustified confidence in data, analysis, predictions and recommendations **A4.2.9** hidden bias, unfair outcomes and inappropriate workplace decisions **A4.2.10** legal, ethical, operational and reputational consequences **A4.3 Advantages** **A4.3.1** insightful and accurate: pattern recognition, anomaly detection, outlier identification **A4.3.2** rapid data cleaning, validation, transformation, integration, sorting, filtering, categorisation, classification, prediction, forecasting, insight generation **A4.3.3** critical interpretation of system-generated patterns, findings, recommendations **A4.3.4** data sources, tools, models, analytical rules and processing methods
A5 Demonstrate understanding of the relationship between data quality issues, analytical approach and limited impact on analysis.	**A5.1 Data quality limitations and conclusions** **A5.1.1** accuracy, completeness, consistency, validity, relevance and timeliness **A5.1.2** sample size, missing variables or groups, geographic or time coverage, outdated data, errors and outliers **A5.1.3** effect on: calculations, comparisons, generalisation, uncertainty and confidence

Pre-Accreditation Draft

Content outcome	Content detail
	A5.1.4 impact of bias, incomplete data, or lack of representativeness **A5.1.5** sample size, missing variables or groups, geographic or time coverage, outdated data, errors, and outliers **A5.1.6** effect on calculations, comparisons, generalisation, uncertainty, and confidence **A5.1.7** uncertainty and confidence in conclusions, the impact of outliers, sampling bias, and unrepresentative data **A5.2 Impacts** **A5.2.1** missing values, incomplete records, absent fields, **A5.2.2** insufficient sampling, unrepresentative or insufficient data **A5.2.3** duplicate records, repeated entries and conflicting versions, conflicting values, mismatched information across sources **A5.2.4** inconsistent formats, data types, units, naming conventions, category definitions **A5.2.5** sampling, selection, measurement, historical and algorithmic bias bias introduced during data collection, preparation, labelling, processing and model development **A5.2.6** inappropriate categories, assumptions and processing rules that exclude or distort valid information **A5.2.7** effects of dataset limitations and bias on patterns, outputs, conclusions and affected groups **A5.2.8** effects on: calculations, comparisons, trends, relationships, conclusions, confidence in analysis
A6 Demonstrate knowledge and understanding of methods used to validate, prepare and determine suitability of data, prior to analysis	**A6.1 Data validation and preparation methods** **A6.1.1** checking: format, data type, presence, range, length and consistency checks, completeness of records, required fields and expected values, valid value ranges, permitted categories, units and date formats

Pre-Accreditation Draft

Content outcome	Content detail
	A6.1.2 ensuring: standardisation of formats, labels, codes, categories and units, resolution of missing, duplicate, inconsistent and conflicting data values **A6.1.3** verifying data against source records, reference data, business rules and documented requirements **A6.2 Determine suitability for analysis** **A6.2.1** relevance to the defined purpose, required fields, level of detail and intended audience **A6.2.2** completeness, accuracy, validity, consistency, timeliness, source credibility and representativeness **A6.2.3** file format, structure, data types, units, metadata, access permissions and compatibility with available tools **A6.2.4** limitations, bias, privacy, confidentiality and risks affecting whether data can be used responsibly **A6.3 Prepare data for analysis** **A6.3.1** inspect fields, records, formats, data types, units and required values before processing **A6.3.2** validating: presence, uniqueness, format, range, code look-up, length, data type, format, consistency against documented rules **A6.3.3** removing: duplicate, inconsistent, invalid, conflicting values **A6.3.4** standardising: labels, codes, categories, units and date formats while preserving source meaning **A6.3.5** confirming completeness, retaining an audit trail of preparation decisions and changes
A7 Demonstrate knowledge and understanding of sustainability considerations relating to the preparation, storage and sharing of data outputs	**Sustainable data practice** **A7.1 Impacts** **A7.1.1** energy use and carbon emissions from devices, networks, servers, cloud services and data centres **A7.1.2** hardware manufacture, replacement and electronic waste

Pre-Accreditation Draft

Content outcome	Content detail
	A7.1.3 storage requirements and network traffic from large datasets and files **A7.2 Sustainable practice** **A7.2.1** collect and process only necessary data; identify errors early and avoid repeated processing **A7.2.2** use suitable hardware, software, automation and local processing efficiently **A7.2.3** retain data only as long as needed; remove obsolete, duplicate and redundant files **A7.2.4** use appropriate storage capacity, file formats and compression without reducing required quality **A7.2.5** share summaries or smaller datasets where sufficient; use links or shared folders instead of duplicate copies **A7.2.6** use digital outputs where appropriate to reduce printing **A7.2.7** storing data sustainably

Pre-Accreditation Draft

Content area B: Analysis, combining datasets and reliable conclusionsContent outcome

Content Outcome	Content detail
B1 Demonstrate knowledge and understanding of analytical techniques used to examine prepared datasets	**B1.1 Applying analytical techniques** **B1.1.1** sort, filter, group and rank records **B1.1.2** calculate totals, averages, percentages, rate of change, and category comparisons using suitable formulas and functions **B1.1.3** use charts, graphs, pivot tables and summary statistics to identify patterns, trends, relationships, variability, anomalies and outliers **B1.1.4** select techniques that suit the data type and analytical purpose; verify calculations against source evidence
B2 Demonstrate knowledge and understanding of how combining datasets from different sources can reveal relationships and insights not visible when sources are analysed separately	**B2.1 Combining datasets** **B2.1.1** link records using reliable common fields and use combined data to add context, reveal relationships and cross-check evidence **B2.1.2** check compatible structures, formats, units, definitions, time periods, completeness, accuracy, privacy and relevance **B2.1.3** recognise risks from mismatched identifiers, definitions or formats, including missing links, duplicates, incorrect calculations and misleading conclusions **B2.1.4** reduce risk through agreed definitions, metadata, mapping, standardisation and documented assumptions
B3 Demonstrate knowledge and understanding of the relationship between data preparation, analytical methods and the reliability of conclusions	**B3.1 Reliability** **B3.1.1** relate preparation quality and method suitability to the strength of conclusions **B3.1.2** consider dataset size, representativeness, missing data, bias, age, outliers and other limitations
B4 Be able to analyse prepared datasets to identify patterns, relationships and trends	**B4.1 Analyse prepared datasets** **B4.1.1** apply suitable sorting, filtering, grouping, ranking, calculations and summary statistics

Pre-Accreditation Draft

	B4.1.2 compare categories and time periods and identify patterns, relationships, trends, anomalies and outliers **B4.1.3** check calculations and outputs against source evidence and the defined analytical purpose
B5 Be able to draw reasoned conclusions from analysed data	**B5.1 Draw reasoned conclusions** **B5.1.1** link conclusions directly to the analysed evidence and defined decision-making purpose **B5.1.2** distinguish correlation from causation and consider alternative explanations **B5.1.3** account for data quality, bias, representativeness, uncertainty and other limitations **B5.1.4** state the strength of evidence, level of confidence and any need for further investigation

Pre-Accreditation Draft

Content area C: Analytical outputs, visualisation and communication

Content outcome	Content detail
C1 Demonstrate knowledge and understanding of the forms and uses of analytical outputs	**C1.1 Forms and uses** **C1.1.1** summaries, comparisons, trends, patterns and performance indicators **C1.1.2** tables, charts, graphs, dashboards, reports, maps, infographics and interactive visualisations **C1.1.3** to support conclusions, make recommendations, inform workplace decision making
C2 Demonstrate knowledge and understanding of how automated visualisation tools may influence interpretation of findings,	**C2.1 Automated visualisation and interpretation** **C2.1.1** automated selection of chart types, scales, ranges, groupings, colours and categories **C2.1.2** scale, proportion, axis intervals and visual emphasis as influences on interpretation **C2.1.3** treatment of outliers, missing values and aggregated data in automated outputs **C2.1.4** the use of AI enabled systems for visualisation
C3 Demonstrate knowledge and understanding of how workplace setting, audience needs and decision-making purpose influence the selection of presentation formats	**C3.1 Workplace purpose, audience and presentation format** **C3.1.1** workplace setting, type of decision being supported **C3.1.2** technical and non-technical audiences, prior knowledge and information needs, accessibility, usability **C3.1.3** level of detail, frequency of use, delivery channel, device and accessibility requirements **C3.1.4** presentation formats suited to exact values, category comparisons, time trends, proportions, relationships, locations and monitoring
C4 Demonstrate knowledge and understanding of principles of visual communication that support accurate,	**C4.1 Accurate, transparent and proportionate visual communication** **C4.1.1** accurate values, consistent scales, proportional representation, clear labels, legends and units

Pre-Accreditation Draft

transparent, proportionate and non-misleading representation of analysed data findings	**C4.1.2** sources, timeframes, calculations, assumptions, limitations and uncertainty **C4.1.3** misleading practices, including truncated axes, distorted images, unnecessary three-dimensional effects, cherry-picking and disproportionate emphasis
C5 Demonstrate knowledge and understanding of the relationship between analytical findings and presentation choices and user interpretation of information	**C5.1 Presentation choices and user interpretation** **C5.1.1** alignment between analytical findings, message, presentation format and audience needs **C5.1.2** effects of layout, sequence, terminology, colour, labelling and level of detail on understanding **C5.1.3** risks of ambiguity, information overload, omitted context and inappropriate visual emphasis
C6 Demonstrate knowledge and understanding of the role of interpretation and professional judgement in transforming analytical results into meaningful conclusions, including distinguishing correlation from meaningful relationships	**C6.1 Interpretation and professional judgement** **C6.1.1** patterns, trends, comparisons, relationships, anomalies and unusual results in context **C6.1.2** correlation, causation, meaningful relationships and alternative explanations **C6.1.3** sufficiency of evidence, reasonable conclusions, confidence, uncertainty and the need for further investigation **C6.1.4** professional, ethical and contextual factors affecting interpretation and conclusions
C7 Be able to interpret a defined analytical and decision-making purpose	**C7.1 Analytical and decision-making** **C7.1.1** identify the question, intended decision, workplace context, audience, required outputs and success criteria **C7.1.2** determine the scope, constraints, assumptions, timescale and level of detail required
C8 Be able to examine analytical outputs in relation to the defined purpose	**C8.1 Examine analytical outputs** **C8.1.1** compare summaries, tables, charts, dashboards and indicators with the defined purpose **C8.1.2** check relevance, accuracy, consistency, scale, proportion, labels, units and supporting context

Pre-Accreditation Draft

C9 Be able to interpret analytical findings and consider potential sources of bias and limitation in the data	**C9.1 Interpret findings, bias and limitations** **C9.1.1** explain patterns, relationships, trends, anomalies and uncertainty in context **C9.1.2** consider sampling, selection, measurement, historical and algorithmic bias and unrepresentative data
C10 Be able to select and apply graphical and tabular visualisation formats to present analysed insights clearly and accurately and inclusively	**C10.1 Select and apply visualisation formats** **C10.1.1** charts, graphs, dashboards, histograms, tables, **C10.1.2** appropriate notation for clarification and accessibility access **C10.2 Inclusive and accessible presentation** **C10.2.1** use clear, concise language, logical structure, meaningful headings and consistent terminology **C10.2.2** use readable fonts, spacing and contrast; do not rely on colour alone **C10.2.3** provide descriptive titles, labels and legends for visualisations and avoid unnecessary complexity **C10.2.4** provide alternative text, captions, transcripts and alternative formats where appropriate **C10.2.5** support screen readers through headings, reading order, structure and descriptive links **C10.2.6** combine formats where useful, prioritise key findings and avoid information overload
C11 Be able to ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations	**C11.1 Assure accuracy and transparency** **C11.1.1** verify displayed values, calculations, labels, units, sources and timeframes **C11.1.2** disclose assumptions, exclusions, limitations, uncertainty
C12 Be able to communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences	**C12.1 Communicate findings and conclusions** **C12.1.1** communicate the message based on purpose, evidence, insight, conclusion and implications of the finding and conclusions **C12.1.2** adapt terminology, detail, format and delivery for technical and non-technical audiences

Pre-Accreditation Draft

C13 Be able to document analytical decisions, assumptions and outputs clearly	**C13.1 Document decisions, assumptions and outputs** **C13.1.1** record data sources, preparation, analytical methods, calculations, tools, assumptions, decisions and versions **C13.1.2** maintain traceability between source data, analysis, findings and presented outputs
C14 Be able to review presented outputs to improve clarity, accessibility and relevance	**C14.1 Review and improve presented outputs** **C14.1.1** check clarity, accuracy, relevance, accessibility, consistency and potential for misleading interpretation **C14.1.2** refine content, layout, labelling, level of detail and alternative formats in response to review findings

Pre-Accreditation Draft

Content area D: Data quality, bias, representativeness and confidence

Content outcome	Content detail
D1 Demonstrate knowledge and understanding of principles of inclusive and unbiased data handling that support fair, accurate and responsible interpretation of analytical findings	**D1.1 Bias and representativeness** **D1.1.1** sampling, selection, non-response, question, measurement, historical and Dalgorithmic bias **D1.1.2** consider whether the sample reflects the relevant population, demographics, locations, time period and user groups **D1.1.3** recognise distorted trends, unfair comparisons, misleading conclusions and inappropriate resource allocation **D1.2 Fair handling** **D1.2.1** use accessible collection methods, respectful categories, balanced samples, multiple credible sources and objective methods **D1.2.2** check, correct or report missing, conflicting, invalid, duplicate, irrelevant and out-of-date data **D1.2.3** present positive and negative findings objectively; separate evidence from interpretation and disclose assumptions, exclusions and uncertainty

Pre-Accreditation Draft

Transferable skills

Students are expected to develop the following transferable skills through the learning and assessment activities for this unit:

- **Analysing** when identifying patterns, relationships and trends within
- datasets and interpreting findings.
- **Decision making** when selecting analytical approaches and drawing
- justified conclusions.
- **Communicating** when presenting insights clearly to technical and nontechnical audiences.

The qualification Delivery Guide suggests ways for centres to help students develop these transferable skills.

Assessment summary

The NEA for this unit consists of five tasks.

- In response to Task 1, students will produce a project plan that identifies the purpose, audience, requirements and outputs, and considers data risks and how governance can manage them.
- In response to Task 2, students will investigate the structure, definitions and metadata of two datasets to report on their suitability, completeness, comparability, quality and privacy risks.
- In response to Task 3, students will combine, clean and manipulate the datasets into a unified data solution and present the data for technical and non-technical audiences.
- In response to Task 4, based on the data solution, students will produce a report that analyses patterns, trends, anomalies and uncertainty to draw conclusions for the defined requirements.
- In response to Task 5, students will evaluate the data solution against the project requirements, justifying selected outputs, identifying limitations and challenges, and recommending improvements.

The assessment will take 15 supervised hours to complete.

The NEA is set by Pearson and will be marked by centres and moderated by Pearson. A new NEA for this unit will be released each September through the secure area of our website. Students must use the assessment to provide the required evidence to achieve this unit.

A sample assessment is provided on the Pearson website.

Pre-Accreditation Draft

Marking the NEA

You will make assessment decisions for the NEA using the marking grid provided below. Before making assessment decisions, you should refer to the guidance on using the marking grid provided in the *Pearson V Levels Supplementary Specification,* available on our website. A glossary of terms used in the marking grid is provided in *Appendix 1*.

Further information on managing NEAs is provided in the *Pearson V Levels Supplementary Specification,* available on our website.

Pre-Accreditation Draft

Marking grid - Unit 1

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 1: Project Plan				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** choice of information from the project scenario has been used to produce a **partial** analysis of the project. Evidenced through: **simplistic** consideration of the purpose and audience with reference to the project scenario **superficial** consideration of the required outputs with reference to the project scenario • **partial** consideration of the data and governance requirements	Appropriate choice of information from the project scenario has been used to produce an **adequate** analysis of the project. Evidenced through: • **appropriate** consideration of the purpose and audience with reference to the project scenario • **sufficient** consideration of the required outputs with reference to the project scenario • **relevant** consideration of the data and governance requirements	**Skilful** choice of information from the project scenario has been used to produce a **secure** analysis of the project. Evidenced through: • **effective** consideration of the purpose and audience with reference to the project scenario • **logical** consideration of the required outputs with reference to the project scenario • **detailed** consideration of the data and governance requirements	**Perceptive** choice of information from the project scenario has been used to produce an **in-depth** analysis of the project. Evidenced through: • **thorough** consideration of the purpose and audience with reference to the project scenario • **insightful** consideration of the required outputs with reference to the project scenario • **comprehensive** consideration of the data and governance requirements

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 2: Suitability of data				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** understanding of the suitability of the supplied data used to produce a **partial** report for the defined purpose. Evidenced through: • **simplistic** investigation into the structure of the data with obvious omissions. • **partial** analysis of the field definitions and values with obvious omissions. • **some** investigation into the characteristics of the metadata with obvious omissions. • **basic** review of the suitability, quality, completeness and comparability of data with obvious omissions.	**Competent** understanding of the suitability of the supplied data used to produce a **clear** report for the defined purpose. Evidenced through: • **sufficient** investigation into the structure of the data with minor omissions. • **coherent** analysis of the field definitions and values with minor omissions. • **suitable** investigation into the characteristics of the metadata with minor omissions. • **adequate** review of the suitability, quality, completeness and comparability of data with minor omissions.	**Effective** understanding of the suitability of the supplied data used to produce a **focused** report for the defined purpose. Evidenced through: • **reasoned** investigation into the structure of the data. • **balanced** analysis of the field definitions and values. • **considered** investigation into the characteristics of the metadata. • **developed** review of the suitability, quality, completeness and comparability of data	**Comprehensive** understanding of the suitability of the supplied data used to produce a **mature** report for the defined purpose. Evidenced through: • **comprehensive** investigation into the structure of the data. • **In-depth** analysis of the field definitions and values. • **insightful** investigation into the characteristics of the metadata. • **critical** review of the suitability, quality, completeness and comparability of data

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 3: Data preparation, manipulation and communication outputs				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** application of relevant techniques to prepare the data ready for analysis and communication. Evidenced through: • **partial** use of suitable data preparation techniques to prepare the datasets for processing • **some** use of appropriate data manipulation methods and techniques to prepare the datasets for analysis • **simplistic** creation of visual output results suitable for technical and/or non-technical audiences	**Clear** application of relevant techniques to prepare the data ready for analysis and communication. Evidenced through: • **sufficient** use of suitable data preparation techniques to prepare the datasets for processing • **suitable** use of appropriate data manipulation methods and techniques to prepare the datasets for analysis • **reliable** creation of visual output results suitable for technical and non-technical audiences	**Confident** application of relevant techniques to prepare the data ready for analysis and communication. Evidenced through: • **effective** use of suitable data preparation techniques to prepare the datasets for processing • **proficient** use of appropriate data manipulation methods and techniques to prepare the datasets for analysis • **detailed** creation of visual output results suitable for technical and non-technical audiences	**Sophisticated** application of relevant techniques to prepare the data ready for analysis and communication. Evidenced through: • **comprehensive** use of suitable data preparation techniques to prepare the datasets for processing • **in-depth** use of appropriate data manipulation methods and techniques to prepare the datasets for analysis • **thorough** creation of visual output results suitable for technical and non-technical audiences

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 4: Analyse findings and draw conclusions				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** evaluation of the findings to produce **simplistic** conclusions Evidenced through: • **imbalanced** analysis of patterns and trends • **partial** analysis of anomalies and uncertainty • **basic** conclusion, if present	**Appropriate** evaluation of the findings to produce **reliable** conclusions Evidenced through: • **competent** analysis of patterns and trends • **sufficient** analysis of anomalies and uncertainty • **coherent** conclusion	**Secure** evaluation of the findings to produce **reasoned** conclusions Evidenced through: • **considered** analysis of patterns and trends • **proficient** analysis of anomalies and uncertainty • **developed** conclusion	**Comprehensive** evaluation of the findings to produce **insightful** conclusions Evidenced through: • **in-depth** analysis of patterns and trends • **critical** analysis of anomalies and uncertainty • **thorough** conclusion

Pre-AccreditationDra

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 5: Recommendations				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	Imbalanced evaluation report of the selected data solution. Evidenced through: • simplistic identification of strengths and weaknesses against the defined project requirements. • some justification of selected outputs. • basic identification of the challenges and limitations of the data solution chosen • partial identification of potential improvements to the data solution, if present	Adequate evaluation report of the selected data solution. Evidenced through: • appropriate identification of strengths and weaknesses against the defined project requirements. • sufficient justification of selected outputs. • coherent identification of the challenges and limitations of the data solution chosen • suitable identification of potential improvements to the data solution	Detailed evaluation report of the selected data solution. Evidenced through: • reasoned identification of strengths and weaknesses against the defined project requirements. • detailed justification of selected outputs. • confident identification of the challenges and limitations of the data solution chosen • convincing identification of potential improvements to the data solution	Comprehensive evaluation report of the selected data solution. Evidenced through: • mature identification of strengths and weaknesses against the defined project requirements. • thorough justification of selected outputs. • concise identification of the challenges and limitations of the data solution chosen • critical identification of potential improvements to the data solution

Please refer to *Pearson V Levels Supplementary Specification* for further guidance on NEAs, including how to apply the marking grids to student evidence .

Pre-Accreditation Draft

Resource requirements

- Appropriate equipment or digital technology for creating, sharing, and saving evidence.

Pre-Accreditation Draft

Unit 2: Securing Digital Systems

Assessment type: Non-exam assessment (NEA)

Unit type: Mandatory

Guided learning hours: 72

Introduction

Every organisation that relies on digital systems relies on someone keeping those systems secure.

In this unit you will develop knowledge and understanding of the threats and issues that affect digital systems, and of the protocols and technologies used to protect them. You will examine preventative and protective actions, including authentication requirements and access controls, and consider how they reduce risk to systems and the information they hold.

You will apply security protocols and interpret system information to detect potential cyber security concerns. You will develop practical skills in security monitoring, recognising when a concern needs to be escalated and how to do so appropriately.

You will communicate your findings and decisions clearly, drawing on evidence from the system information you have interpreted to justify the actions you recommend.

Students should be given opportunities to develop their knowledge and skills in a range of contexts including different platforms, physical environments, policies and scenarios.

Pre-Accreditation Draft

Teaching content

Content area A: Understanding security requirements and threats

Content outcome	Content detail
A1 Demonstrate knowledge and understanding of authentication requirements.	**A1.1** Authentication verifies identity; authorisation determines permitted actions; access control enforces decisions across accounts, devices, applications, services and data. **A1.2** Authentication requirements including: **A1.2.1** credentials, multifactor authentication (MFA), **A1.3** Factors determining the required strength of authentication: **A1.3.1** sensitivity of the system or data, exposure, consequence of compromise **A1.4** Role-based access control (RBAC): access based on a user's role in the organisation, as applied when setting up accounts and permissions, least privilege. **A1.5** Least privilege: limiting each user and service to the minimum access needed for authorised activity, reducing accidental and malicious impact while supporting accountability. **A1.6** Relate update and data protection measures to vulnerability reduction and to the CIA triad: confidentiality, integrity and availability. **A1.7** Judge trade-offs between control strength, usability, accessibility, continuity and risk when planning which measures to apply. **A1.8** relationship between authentication strength, usability and security risk
A2 Demonstrate knowledge and understanding of policies relating to secure practice.	**A2.1** Policy defines authorised behaviour, responsibilities and escalation routes; procedure translates policy into consistent operational action. **A2.2** Policy types, including: **A2.2.1** acceptable use, access control, data-handling policy - rules governing storage, sharing, retention and disposal, incident reporting **A2.3** Incident response procedure stages: **A2.3.1** initial decision, triage and escalation **A2.3.2** response, analysis, containment and mitigation **A2.3.3** reporting and escalation of suspected security incidents **A2.4.4** Secure practice considerations

Pre-Accreditation Draft

Content outcome	Content detail
	A2.4.1 acceptable use of systems, devices and services, **A2.3.5** user authentication and access permissions **A2.3.6** secure storage, sharing and disposal of data
A3 Demonstrate knowledge and understanding of common cyber security threats.	**A3.1** Threat types, including: **A3.1.1** phishing, social engineering, malware, ransomware, unauthorised access attempts, suspicious network behaviour, data loss incidents **A3.2** Distinguish a threat from a vulnerability, an indicator, an event and an incident **A3.3** Relate a threat to its likely route: **A3.3.1** user behaviour, account compromise, software, network services, data handling, gaps in existing controls **A3.4** Assess likely impact and urgency from the devices affected, exposure, persistence, scale and potential harm **A3.5** Prioritise risks as low, medium or high

Pre-Accreditation Draft

Content area B: Applying security controls

Content outcome	Content detail
B1 Be able to apply application update and data protection measures to digital systems.	**B1.1** Configure credentials on a supplied system **B1.2** Configure access controls on a supplied system, including: **B1.2.1** account permissions **B1.2.2** user groups and group membership **B1.3** Authentication requirements **B1.3.1** example of authentication requirements **B1.4** Data protection measures **B1.4.1** data protection measures **B1.4.2** least privilege **B1.5** Verifying and recording configuration changes **B1.5.1** Check settings have taken effect **B1.5.2** Record what was changed, and why **B1.6** Configuring wireless security on a wireless access point, including: **B1.6.1** wireless encryption and passphrase **B1.6.2** network name (SSID) settings **B1.6.3** limiting the number of devices that can connect **B1.7** Reducing the attack surface of end-user devices and servers.
B2 Demonstrate configuration actions in line with defined security procedures	**B2.1** Configure user accounts and permissions **B2.1.1** Create user accounts and permissions **B2.1.2** Amend user accounts and permissions **B2.1.3** Remove user accounts and permissions **B2.2** Apply security settings, including: **B2.2.1** password policy, lockout thresholds, device or service restrictions **B2.3** Check configuration against given requirements **B2.3.1** Passwords, Access controls, Least privilege,

Pre-Accreditation Draft

B3 Demonstrate procedures for secure access, authentication and system use	**B3.1** Secure day-to-day system use **B3.1.1** Log in and out of a system correctly. **B3.1.2** Use authentication as required. **B3.1.3** Do not bypass or disable controls for convenience.
B4 Demonstrate knowledge and understanding of energy, data retention and secure lifecycle practices	**B4.1** Switching off unused ports, services and devices to reduce energy use and opportunities for attack. **B4.2** Data-retention management: **B4.2.1** what security information is kept, purpose, duration, location, responsibility **B4.3** Secure device lifecycle practices relevant to monitoring and access: **B4.3.1** procurement and configuration **B4.3.2** supported updates and an up-to-date inventory of approved devices so that unknown devices can be recognized **B4.3.3** removing access and accounts that are no longer needed **B4.3.4** data cleansing, reuse and disposal

Pre-Accreditation Draft

Content area C: Monitoring and recording security information

Content outcome	Content detail
C1 Demonstrate knowledge and understanding of potential cyber security concern indicators	**C1.1** Security information sources: **C1.1.1** logs: time-ordered records of events **C1.1.2** alerts: activity matching defined rules or models **C1.1.3** account records: access, authentication and privilege activity **C1.2** Indicators of potential concern, including: **C1.2.1** repeated failures, unusual times or locations, privilege changes, unfamiliar devices, anomalous data transfer, blocked actions, unexpected service activity, access from an unexpected network or IP address range **C1.3** Correlating evidence across sources **C1.3.1** Correlate identity, time, source, destination, action and outcome across more than one source. **C1.3.2** Use correlation to strengthen or weaken a possible concern, rather than relying on a single entry in isolation. **C1.4** Distinguishing normal variation from anomaly **C1.4.1** Use supplied baseline data, context and corroborating evidence to judge whether activity is normal or anomalous. **C1.4.2** Record uncertainty rather than drawing a conclusion from an isolated event **C1.4.3** Classify activity as normal, uncertain or a concern.
C2 Be able to review security-related information that indicates system quality issues	**C2.1** System-quality indicators **C2.1.1** Identify slow response times from supplied dashboard or log data. **C2.1.2** Identify repeated errors from supplied dashboard or log data. **C2.1.3** Identify failed updates from supplied dashboard or log data. **C2.1.4** Identify connectivity interruptions from supplied dashboard or log data. **C2.1.5** Distinguish system-quality issues from security concerns, recognizing that they can be related.

Pre-Accreditation Draft

C3 Be able to recognise signs of unexpected and anomalous system activity	**C3.1** Signs of unexpected or anomalous activity: **C3.1.1** volume - unusually high or low numbers of events, logins, connections, alerts or data transferred **C3.1.2** timing - activity outside normal working hours, at an unusual frequency, or in an unexpected order **C3.1.3** source - activity from unfamiliar accounts, devices, IP address ranges or locations **C3.1.4** type - actions not normally seen on the system **C3.2** Procedures for recognising unexpected and anomalous activity**:** **C3.2.1** establishing expected activity from policies, baseline, data, or system documentation **C3.2.2** comparing observed activity with a baseline by volume, timing, source, and type **C3.2.3** checking for an authorised explanation **C3.2.4** corroborating a possible anomaly with a second source of security information **C3.2.5** flagging activity that cannot be explained for further judgement, in line with procedure
C4 Be able to use log files, monitoring dashboards and system alerts to view and interpret security-related information	**C4.1** Using logs, dashboards and alerts **C4.1.1** Navigate and read the specific log, dashboard and alert formats supplied for the task. **C4.2** Extract the fields relevant to a security review, including: **C4.2.1** timestamp , source, account, action, outcome
C5 Be able to record observations clearly and accurately	**C5.1** Recording observations **C5.1.1** Produce a record of observations that is clear and accurate. **C5.1.2** Produce a record that is chronological. **C5.1.3** Make use of source evidence.

Pre-Accreditation Draft

Content area D: Judging security concerns and applying protective action

Content outcome	Content detail
D1 Demonstrate knowledge and understanding of the relationship between system activity, security-related information and potential cyber security concerns, including uncertainty in interpretation and the need for professional judgement	**D1.1** The relationship between activity, information and concern **D1.1.1** System activity is the observed behaviour. **D1.1.2** Security information is the recorded or inferred evidence of that activity. **D1.1.3** A concern is a reasoned judgement that activity may threaten confidentiality, integrity or availability. **D1.2** Factors affecting interpretation, including: **D1.2.1** completeness of the evidence, timestamp accuracy, logging scope, baseline quality, context, the possibility of a legitimate explanation **D1.3** Applying professional judgement **D1.3.1** Consider possible explanations for evidence. **D1.3.2** Assess the strength and reliability of evidence **D1.3.3** Determine proportionate next action within personal authority. **D1.3.4** Determine certainty or uncertainty based on available evidence
D2 Demonstrate knowledge and understanding of the role of baseline system behaviour in identifying deviations and potential threats	**D2.1** Baseline system behaviour **D2.1.1** A baseline describes expected users, devices, services, volumes, timings, locations, access patterns and performance ranges for a defined context. **D2.1.2** Use the supplied baseline as the comparison point for judging deviation. **D2.1.3** Judge whether a deviation reflects authorised change, normal operational variation, a fault or a potential threat. **D2.1.4** Investigate to find evidence before treating concerns.

Pre-Accreditation Draft

D3 Demonstrate knowledge and understanding of the relationship between security controls, user behaviour and system vulnerabilities	**D3.1 Controls, behaviour and vulnerabilities** **D3.1** Security controls: **D3.1.1** authentication (passwords, MFA), access controls and permissions, least privilege, software updates and patching, firewalls, encryption, logging and monitoring, backups. **D3.2** Vulnerabilities: **D3.2.1** weak or default passwords, unpatched software, excessive or unnecessary permissions, unused accounts, open ports and services, misconfigured settings, unencrypted data, gaps in logging or monitoring: **D3.3** User behaviours that strengthen controls: **D3.3.1** following policy and procedure, protecting credentials, applying updates, promptly, reporting concerns, suspicious activity. **D3.4** User behaviours that weaken controls: **D3.4.1** credential sharing, unsafe handling of data, ignored updates, insecure workarounds
D4 Demonstrate knowledge and understanding of the implications of different types of cyber threats and the impact of delayed identification and escalation	**D4.1** Implications of threats, including: **D4.1.1** confidentiality, integrity and availability, privacy, finance, reputation, legal compliance, user safety and operational continuity **D4.2** Timing of identification and escalation **D4.2.1** Delayed identification can increase response time, spread and evidence loss, **D4.2.2** Delayed escalation can prevent timely, authorised containment. **D4.2.3** Premature or incorrect escalation can disrupt services and expose information. **D4.2.4** Escalation decisions must be timely, proportionate and evidence-led.

Pre-Accreditation Draft

D5 Demonstrate knowledge and understanding of the importance of accurate interpretation of system information, awareness of false positives and misinterpretation of automated alerts, and the limitations of automated and AI-enabled detection systems	**D5.1** Accurate interpretation of system information **D5.1.1** Separate observed fact from automated classification. **D5.1.2** Separate automated classification from personal inference. **D5.1.3** Separate personal inference from confirmed outcome. **D5.2** False positives, false negatives and alert quality **D5.2.1** A false positive is a benign event flagged as concerning. **D5.2.2** A false negative is a concerning event that is not detected. **D5.3** Limitations of automated and AI-enabled detection systems
D6 Demonstrate knowledge and understanding of the role of automated and AI-enabled detection systems in identifying potential cyber security concerns, and the need to interpret, validate and act on outputs appropriately	**D6.1** The role of automated and AI-enabled detection **D6.1.1** aggregate events, identify patterns, prioritise alerts, highlight deviations. **D6.2** Use of AI outputs to support decision-making
D7 Be able to select and apply protective actions to systems in response to identified risks and system information	**D7.1** Selecting protective action **D7.1.1** Select protective action proportionate to the identified risk. **D7.1.2** Select protective action within personal authority (for example changing a permission, disabling an account, tightening a setting). **D7.1.3** Use the supplied procedures as the governing basis for the action selected. **D7.2** Applying protective action **D7.2.1** Apply the action in a controlled and repeatable way. **D7.2.2** Preserve evidence of the state before and after the action. **D7.2.3** Record the outcome so its effect can be checked.

Pre-Accreditation Draft

Content area E: Escalating concerns and concluding the response

Content outcome	Content detail
E1 Demonstrate knowledge and understanding of policies and procedures relating to privacy, confidentiality and responsible handling of security-related information: storing information securely, restricting access to authorised users, transmitting information appropriately and reporting concerns through defined procedures	**E1.1** Security-related information may contain, and requires controlled handling of: **E1.1.1** personal data, credentials, vulnerability details, system details, incident evidence **E1.2** Handling security-related information securely **E1.2.1** Apply data minimisation, role-based access, approved communication channels, keep accurate records. **E1.3** Reporting through a defined route **E1.3.1** avoiding copying sensitive material unnecessarily, without altering evidence, maintaining confidentiality.

Pre-Accreditation Draft

E2 Be able to escalate potential cyber security concerns in line with security procedures	**E2.1** Escalating a concern **E2.1.1** Recognise the limits of own role and authority **E2.1.2** Identify concerns outside of control or personal authority. **E2.2** Content of an escalation communication **E2.2.1** State the concern. **E2.2.2** Provide supporting evidence. **E2.2.3** Identify next steps. **E2.2.4** Only disclose relevant information. **E2.3** Incident record and report structure, including: **E2.3.1** Concise summary of concerns suitable for audience. **E2.3.2** What was found and how (the investigation). **E2.3.3** The urgency and likely impact. **E2.3.4** mitigations or action already taken **E2.3.5** recommendations and any outstanding risk **E2.4** Drawing conclusions about **E2.4.1** the significance and priority of activities. **E2.4.2** the effectiveness of controls or actions taken. **E2.4.3** the likely impact of a delayed or absent response. **E2.4.4** the quality of evidence that could be uncertain or unreliable. **E2.5** Recommending further action **E5.2.1** continued monitoring, further protective action, further escalation, evidence preservation, process improvement
E3 Be able to communicate potential security concerns clearly to others	**E3.1** Communicating clearly to others **E3.1.1** appropriate language, conciseness, providing relevant information in appropriate format, priority information first, listing actions taken

Pre-Accreditation Draft

E4 Be able to handle security-related information in line with policies and procedures for privacy and confidentiality	**E4.1** Handling security-related information: **E4.1.1** secure storage of information **E4.1.2** restrict user access to information **E4.1.3** appropriate sharing and transmission of information **E4.1.4** confidential disposal of information **E4.2** Protecting privacy and confidentiality: **E4.2.1** redacting or masking personal data and credentials **E4.2.2** labelling information by sensitivity **E4.2.3** filename protocols **E4.2.4** least privilege.

Pre-Accreditation Draft

Transferable skills

Students are expected to develop the following transferable skills through the learning and assessment activities for this unit:

- **Decision making** when selecting actions and escalation routes in line with defined security procedures.
- **Investigative skills**, demonstrated through interpreting system information and monitoring outputs to identify unusual or anomalous behaviour.
- **Communicating** when reporting observations and potential concerns clearly.

The qualification Delivery Guide suggests ways for centres to help students develop these transferable skills.

Assessment summary

The NEA for this unit consists of five tasks.

- In response to Task 1, students will apply knowledge and understanding of threats, vulnerabilities, authentication, access control and policy to identify and prioritise the security risks to a defined organisational network.
- In response to Task 2, students will plan a proportionate, requirements-led security response to the risks they have identified, including user accounts and permissions based on least privilege.
- In response to Task 3, students will configure and apply authentication, access, permission and data protection measures to a simulated network in a controlled environment. They will check and record that each control has taken effect.
- In response to Task 4, students will use supplied events, logs and baseline data to identify, classify and accurately record activity as normal, uncertain or a concern. They will identify any concerns that are outside their authority.
- In response to Task 5, students will escalate a security concern accurately and confidentially through a defined escalation procedure, assessing its urgency and likely impact. They will recommend proportionate next steps and draw conclusions.

The assessment will take 15 supervised hours to complete.

The NEA is set by Pearson and will be marked by centres and moderated by Pearson. A new NEA for this unit will be released each September through the secure area of our website. Students must use the assessment to provide the required evidence to achieve this unit.

A sample assessment is provided on the Pearson website.

Pre-Accreditation Draft

Marking the NEA

You will make assessment decisions for the NEA using the marking grid provided below. Before making assessment decisions, you should refer to the guidance on using the marking grid provided in the *Pearson V Levels Supplementary Specification,* available on our website. A glossary of terms used in the marking grid is provided in *Appendix 1*.

Further information on managing NEAs is provided in the *Pearson V Levels Supplementary Specification,* available on our website..

Pre-Accreditation Draft

Marking grid

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 1: Identify security risks				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** application of knowledge and understanding of the threats and vulnerabilities in the supplied network and scenario. Evidenced through **superficial** risk identification that: • identifies a few vulnerabilities in the network, with **partial** links to the devices, accounts, or data affected • gives **simplistic** reasons why threats might occur • prioritises risks through an **imbalanced** assessment of likelihood and impact.	**Adequate** application of knowledge and understanding of the threats and vulnerabilities in the supplied network and scenario. Evidenced through **appropriate** risk identification that: • identifies the main vulnerabilities in the network, with **clear** links to the devices, accounts, and data affected • gives **relevant** reasons why threats might occur • prioritises risks through a **coherent** assessment of likelihood and impact.	**Secure** application of knowledge and understanding of the threats and vulnerabilities in the supplied network and scenario. Evidenced through **considered** risk identification that: • identifies most vulnerabilities across the network, with **accurate** links to the devices, accounts, and data affected • gives **logical** reasons why threats might occur • prioritises risks through a **balanced** assessment of likelihood and impact.	**Comprehensive** application of knowledge and understanding of the threats and vulnerabilities in the supplied network and scenario. Evidenced through **in-depth** risk identification that: • identifies the full range of vulnerabilities across the network, with **thorough** links to the devices, accounts, and data affected • gives **sophisticated** reasons why threats might occur • prioritises risks through a **insightful** assessment of likelihood and impact.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 2: Plan the secure response				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** application of knowledge and understanding to plan a secure response to the identified risks. Evidenced through a **partial** plan that: proposes security controls, user groups and permissions with **occasional** links to the identified risks and least privilege sets out a sequence of actions with **obvious** gaps or errors includes **simplistic** methods for checking that each control has worked gives **superficial** justification of why controls are proportionate to the level of risk.	**Appropriate** application of knowledge and understanding to plan a secure response to the identified risks. Evidenced through a **relevant** plan that: proposes security controls, user groups and permissions that are **mostly** linked to the identified risks and least privilege sets out a sequence of actions with **minor** gaps or errors includes **reliable** methods for checking that each control has worked gives **clear** justification of why controls are proportionate to the level of risk.	**Effective** application of knowledge and understanding to plan a secure response to the identified risks. Evidenced through a **logical** plan that: proposes security controls, user groups and permissions that are **consistently** linked to the identified risks and least privilege sets out a **considered** sequence of actions includes **pertinent** methods for checking that each control has worked gives **convincing** justification of why controls are proportionate to the level of risk.	**Comprehensive** application of knowledge and understanding to plan a secure response to the identified risks. Evidenced through a **thorough** plan that: proposes security controls, user groups and permissions that are **fully** linked to the identified risks and least privilege sets out a **sophisticated** sequence of actions includes **in-depth** methods for checking that each control has worked gives **perceptive** justification of why controls are proportionate to the level of risk.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 3: Apply security controls				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** application of knowledge and understanding of security controls. Evidenced through **inconsistent** configuration that: • **some** removal of vulnerabilities in the network • shows **emerging** application of least privilege to user groups, accounts and permissions • is **partially** checked and recorded, with **uneven** evidence that controls have taken effect.	**Competent** application of knowledge and understanding of security controls. Evidenced through **sound** configuration that: • **adequate** removal of vulnerabilities in the network • shows **adequate** application of least privilege to user groups, accounts and permissions • is **clearly** checked and recorded, with **sufficient** evidence that controls have taken effect.	**Effective** application of knowledge and understanding of security controls. Evidenced through **secure** configuration that: • **effective** removal of vulnerabilities in the network • shows **consistent** application of least privilege to user groups, accounts and permissions • is **proficiently** checked and recorded, with **pertinent** evidence that controls have taken effect.	**Comprehensive** application of knowledge and understanding of security controls. Evidenced through **fluent** configuration that: • **thorough** removal removes vulnerabilities in the network • shows **sustained** application of least privilege to user groups, accounts and permissions • is checked and recorded in an **accomplished** way, with evidence confirming that every control has taken effect.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 4: Monitor and record security information				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** review of security information. Evidenced through a **partial** monitoring record that: **partially** classifies a few events accurately makes **literal** comparisons with baseline data, with **superficial** links between data sources gives **simplistic** reasons for each classification **inconsistently** identifies the concerns that are outside own authority.	**Competent** review of security information. Evidenced through a **clear** monitoring record that: **mostly** classifies the majority of events accurately makes **straightforward** comparisons with baseline data, with **coherent** links between data sources gives **relevant** reasons for each classification **appropriately** identifies the concerns that are outside own authority.	**Effective** review of security information. Evidenced through a **reasoned** monitoring record that: **proficiently** classifies most events accurately makes **considered** comparisons with baseline data, with **convincing** links between data sources gives **detailed** reasons for each classification identifies the concerns that are outside own authority in a **focused** way.	**Comprehensive** review of security information. Evidenced through a **sophisticated** monitoring record that: • **Thoroughly** classifies all events accurately, with minor omissions makes **in-depth** comparisons with baseline data, with **insightful** links between data sources gives **perceptive** reasons for each classification **thoroughly** identifies the concerns that are outside own authority.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 5: Escalate and communicate				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Simplistic** escalation and communication of a security concern. Evidenced through a **basic** escalation report that: follows the escalation procedure **inconsistently**, including the handling of confidential information provides an **uneven** summary of the concern, the evidence and any initial action taken assesses urgency and likely impact **partially** makes recommendations with **superficial** links to the evidence.	**Appropriate** escalation and communication of a security concern. Evidenced through a **clear** escalation report that: follows the escalation procedure **soundly**, including the handling of confidential information provides a **relevant** summary of the concern, the evidence and any initial action taken assesses urgency and likely impact **coherently** makes recommendations with **competent** links to the evidence.	**Effective** escalation and communication of a security concern Evidenced through a **confident** escalation report that: follows the escalation procedure **consistently**, including the handling of confidential information provides an **accurate** summary of the concern, the evidence and any initial action taken assesses urgency and likely impact in a **balanced** way makes recommendations with **pertinent** links to the evidence.	**Comprehensive** escalation and communication of a security concern. Evidenced through a **concise** escalation report that: follows the escalation procedure **fully**, including the handling of confidential information provides a **thorough** summary of the concern, the evidence and any initial action taken assesses urgency and likely impact in a **nuanced** way, qualified where evidence is uncertain makes prioritised recommendations with **perceptive** links to the evidence.

Please refer to *Pearson V Levels Supplementary Specification* for further guidance on NEAs, including how to apply the marking grids to student evidence.

Pre-Accreditation Draft

Resource requirements

Students must have the following equipment for the assessment of this unit:

- Appropriate equipment or digital technology for creating, sharing, and saving evidence
- The most recent version of Cisco Packet Tracer, used throughout this unit for network security configuration tasks.

Pre-Accreditation Draft

Unit 3: Configuring Digital Systems

Assessment type: Non-exam assessment (NEA)

Unit type: Optional

Guided learning hours: 72

Introduction

Reliable digital systems depend on careful preparation, controlled configuration and structured testing. In this unit, students interpret requirements, configure a system safely, record decisions and compare observed outcomes with expected outcomes. They use logs, alerts, performance indicators and user feedback to identify deviations, apply structured fault-finding and make an evidence-based readiness judgement. Activities may take place in realistic, controlled, non-live, simulated or training environments.

Students prepare and configure digital systems in response to defined user and system requirements. They apply configuration settings, test system functionality, performance, stability, usability, accessibility and security-related behaviours, correct identified issues and use evidence to determine whether systems are ready for use.

Students should be given opportunities to develop their knowledge and skills in a range of contexts including different systems configurations, software environments, user requirements and work-related scenarios.

Pre-Accreditation Draft

Teaching content

Content area A: Planning configuration and testing

Content outcome	Content detail
A1 Demonstrate knowledge and understanding of the purpose of testing digital systems and the role of quality assurance	**A1.1 Testing and quality assurance** **A1.1.1** comparing observed system behaviour with requirements and expected outcomes **A1.1.2** maintaining system performance, security and reliability
A2 Demonstrate knowledge and understanding of policies relating to data protection, privacy and acceptable system use, and their role in guiding configuration practice.	**A2.1 Policy areas** **A2.1.1** data protection, privacy and acceptable use **A2.1.2** access permissions, user account management with each user responsible for their own account **A2.1.3** secure configuration, updates and safe starting settings **A2.1.4** protection of personal and sensitive information. **A2.1.5** acceptable use of systems, devices and services
A3 Demonstrate knowledge and understanding of the role of workplace policies, standards and compliance requirements in defining testing scope and quality assurance expectations	**A3.1 Workplace requirements** **A3.1.1** policy as mandatory organisational practice **A3.1.2** standards to be met and consistent criteria for configuration and testing **A3.1.3** compliance requirements and the need to evidence compliance **A3.1.4** how to define test scope, data use and acceptance criteria
A4 Demonstrate knowledge and understanding of the role of controlled, non-live, simulated and training environments in supporting safe and effective configuration practice	**A4.1 Configuration environments** **A4.1.1** why controlled, non-live, simulated and training environments are needed to observe how a system behaves without risk **A4.1.2** how these environments protect users, live data and operational services **A4.1.3** how testing settings first helps you get the configuration right before it affects real users

Pre-Accreditation Draft

Content outcome	Content detail
A5 Be able to interpret user and system requirements to determine configuration needs and the scope and focus of testing	**A5.1 Requirements and test scope** **A5.1.1** where requirements come from: user needs, the scenario, information about the system, and policies **A5.1.2** how to turn a requirement into a configuration need, for example "the receptionist needs a screen reader" becomes "install and enable accessibility settings" **A5.1.3** how to write a requirement so it can be tested, with a clear expected result **A5.1.4** how to decide what is in and out of scope for testing **A5.1.5** how to choose what to test first, based on user need, dependencies and risk
A6 Be able to apply policies relating to configuration and data protection requirements: secure configuration, access permissions.	**A6.1 Policy requirements** **A6.1.1** secure configuration requirements **A6.1.2** authorised access permissions **A6.1.3** protection of personal information **A6.1.4** supported software updates **A6.1.5** records showing how configuration meets policy

Pre-Accreditation Draft

Content area B: Preparing and configuring digital systems

Content area B:	Content detail
B1 Demonstrate knowledge and understanding of how system dependencies and component compatibility ensure reliable system operation	**B1.1 Dependencies and compatibility** **B1.1.1** dependencies between services, components, accounts, settings and network resources **B1.1.2** compatibility of versions, platforms, drivers and requirements **B1.1.3** prerequisites and upstream or downstream effects (what must work first, and what depends on it) **B1.1.4** effects on authentication, connectivity, storage, applications and security settings
B2 Demonstrate knowledge and understanding of the impact of system configuration on performance efficiency and resource utilisation	**B2.1 Performance and resources** **B2.1.1** how to set power plans, sleep and screen-off times, and how these impact energy usage, processor, memory, storage, network bandwidth and energy **B2.1.2** how to find and manage startup programs and background apps **B2.1.3** how to read processor, memory and disk use resource monitoring tool **B2.1.4** understand the trade-offs between performance, security, accessibility and efficiency
B3 Demonstrate knowledge and understanding of the role of digital tools in supporting system preparation, configuration and checking activities	**B3.1 Digital tool functions** **B3.1.1** preparing accounts, network, storage, software, updates, security and device settings **B3.1.2** checking configuration status and collecting evidence **B3.1.3** selection of authorised, compatible tools suited to the required control **B3.1.4** verification of settings applied manually or automatically

Pre-Accreditation Draft

B4 Demonstrate knowledge and understanding of the impact of responsible, inclusive and secure configuration practices.	**B4.1 Responsible, inclusive and secure configuration** **B4.1.1** supporting diverse users, reducing barriers to digital participation **B4.1.2** identifying which user needs apply: visual, motor, auditory, cognitive, linguistic **B4.1.3** secure settings that reduce avoidable data exposure **B4.1.4** accessible settings that reduce barriers without unnecessarily weakening security **B4.1.5** recording justified decisions where security and access needs interact
B5 Demonstrate knowledge and understanding of environmental and sustainability considerations associated with system performance and efficient use of digital resources	**B5.1 Sustainability considerations** **B5.1.1** energy use, device lifespan, storage demand, network demand and electronic waste **B5.1.2** efficient software and resource use **B5.1.3** power management, sleep, power-off and process time limits where appropriate
B6 Demonstrate knowledge and understanding of the importance of maintaining system integrity through responsible updates, permissions and security settings	**B6.1 System integrity** **B6.1.1** how to ensure that supported updates are applied that address known weaknesses **B6.1.2** permissions and security settings allow or restrict access to tools and settings
B7 Be able to prepare and configure digital systems to meet defined needs	**B7.1 System preparation and configuration** **B7.1. 1** checking the starting state and access to the environment **B7.1.2** gathering authorised tools, resources and configuration information **B7.1.3** accounts, permissions, organisation-wide settings, connectivity, storage, updates, security and accessibility as required **B7.1.4** recording the resulting configuration

Pre-Accreditation Draft

B8 Be able to adjust configuration settings relating to user access, connectivity, storage and security to support system functionality and accessibility	When considering the policies and safe working practices, user access, connectivity, storage and security, students must draw on content from Unit 2, Securing Digital Systems, section D1, which details the relationship between system activity, security-related information and potential cyber security concerns, including uncertainty in interpretation and the need for professional judgement. **B8.1 User access** **B8.1.1** create standard and administrator accounts, password rules and multi-factor authentication, folder and file permissions,automatic screen lock and sign-in options, find and remove unused or guest accounts. **B8.2 Connectivity** **B8.2.1** wired, Wi-Fi network, private or public network profile, automatic and fixed IP settings, DNS and proxies work, connecting and sharing printers, remote access or Bluetooth needs. **B8.3 Storage** **B8.3.1** check space, storage division, save locations, organise folders, setting up backups or cloud sync, storage limits and temporary file clean-up, drive encryption. **B8.4 Security** **B8.4.1** firewall set allow and block rules, antivirus and real-time protection, scheduling scans, automatic updates and security patches, control app permissions and browser security settings, restrict USB and removable media **B8.5 Software and updates** **B8.5.1** install and remove approved software, default apps and browsers, update schedule and restart times, software versions and compatibility **B8.6. Accessibility** **B8.6.1** text size, contrast, scaling,colour filters and screen readers **B8.6.2** change keyboard, mouse and speech input options **B8.6.3** set language and region

Pre-Accreditation Draft

B9 Be able to maintain system integrity through responsible configuration practices, updates, permissions and security settings	**B9.1 Maintaining integrity** **B9.1.1** set the system to accept system updates **B9.1.2** set minimum required permissions or user group rules **B9.1.3** enable appropriate security settings

Content area C: Testing functionality, performance, usability and security

Content outcome	Content detail
C1 Demonstrate knowledge and understanding of categories of testing used in workplace contexts that address system functionality, performance, usability, accessibility and security-related behaviours	When displaying security related behaviours students must draw on content from Unit 2 Securing Digital Systems, sections A1, D1 and E1, which detail the security-related information, usability and security risk, and principles of least privilege. **C1.1 Testing categories** **C1.1.1** functionality, performance, usability, accessibility and security-related behaviour **C1.1.2** distinct test conditions, inputs, expected outcomes and acceptance criteria for each category **C1.1.3** selection based on system purpose, user needs and risk **C1.1.4** recognition that passing one category does not assure another
C2 Demonstrate knowledge and understanding of principles of usability and accessibility and their relevance to system performance,	**C2.1 Usability and accessibility** **C2.1.1** usability: effectiveness, efficiency and satisfaction in use **C2.1.2** accessibility: ability of diverse users to perceive, operate and understand the system **C2.1.3** layout, navigation, feedback, error messages and input methods **C2.1.4** assistive technology, interaction patterns, user effectiveness **C2.1.5** relationships with interface, support needs, performance, reliability, errors, and security

Pre-Accreditation: Draft

C3 Demonstrate knowledge and understanding of the contribution of inclusive and accessible testing practices to reliable digital systems for diverse users	**C3.1 Inclusive testing** **C3.1.1** success criteria derived from stated access needs **C3.1.2** representative tasks, input methods, devices and settings **C3.1.3** accessibility findings recorded consistently with other findings **C3.1.4** limits of functional checks when identifying barriers
C4 Demonstrate knowledge and understanding of the role of contemporary digital tools in supporting test planning, identification of patterns in system behaviour and summarisation of findings	**C4.1 Tools supporting testing** **C4.1.1** planning tests and maintaining traceability **C4.1.2** recording and comparing results **C4.1.3** reviewing logs and identifying patterns **C4.1.4** summarising findings **C4.1.5** checking summaries against source information
C5 Demonstrate knowledge and understanding of the role of digital tools and automated and AI-enabled systems in supporting system configuration, testing and identification of patterns in system behaviour, and the need to review outputs to ensure accuracy and suitability	**C5.1 Automated and AI-enabled support** **C5.1.1** suggesting settings, generating checks, classifying events, identifying patterns and summarising results **C5.1.2** dependence of output quality on data, instructions and system rules **C5.1.3** comparison of outputs with requirements and observed behaviour **C5.1.4** human oversight, verification and accountability for decisions
C6 Be able to carry out structured tests to confirm system functionality, performance, stability and security-related behaviours	**C6.1 Structured testing** **C6.1.1** test condition, input, expected outcome and acceptance criteria **C6.1.2** logical sequence based on dependencies and risk **C6.1.3** evidence from observations, logs, alerts, screenshots and performance indicators **C6.1.4** pass or fail decisions against defined criteria

Pre-Accreditation Draft

C7 Be able to assess system usability and accessibility against stated user needs	**C7.1 Usability and accessibility assessment** **C7.1.1** representative user tasks **C7.1.2** ease and effectiveness of task completion **C7.1.3** accessibility settings and stated needs **C7.1.4** observation, task results and user feedback **C7.1.5** distinction between user preference and defined requirement
C8 Be able to apply routine checks to confirm systems are ready for use. , connectivity and network access, storage availability, software updates and security settings, expected system functionality and performance	**C8.1 Routine readiness checks** **C8.1.1** user access and authentication - test sign-in and permissions **C8.1.2** connectivity and network access - check a network connection works **C8.1.3** check the amount of storage available **C8.1.4** software updates and security settings - check firewall, updates and antivirus status **C8.1.5** expected functionality and performance – use system monitoring tools to status of hardware, software and resources **C8.1.6** repeat checks after relevant changes - record settings before and after a change

Pre-Accreditation Draft

Content area D: Reviewing system behaviour and correcting faults

Content outcome	Content detail
D1 Demonstrate knowledge and understanding of methods used to assess system behaviour through comparison of observed outputs with expected outcomes, interpretation of system logs, alerts and performance indicators, and identification of patterns and recurring issues	**D1.1 Assessment methods** **D1.1.1** comparison of observed outputs with requirements, expected outcomes or baseline behaviour **D1.1.2** interpretation of system logs, alerts and performance indicators **D1.1.3** identification of deviations, symptoms, patterns and recurring issues **D1.1.4** distinction between telling what happened from why it happened
D2 Demonstrate knowledge and understanding of the impact of system performance, reliability and security issues on user experience, productivity and service continuity	**D2.1 Impact of system issues** **D2.1.1** performance, reliability and security issue types **D2.1.2** effects on user experience, productivity and service continuity **D2.1.3** severity, duration, users affected, data sensitivity and available workarounds **D2.1.4** priority based on organisational and user impact
D3 Be able to review system behaviour and outputs to identify deviations from expected outcomes and apply structured fault-finding approaches where required	**D3.1 Structured fault-finding** **D3.1.1** defining the symptom and expected behaviour **D3.1.2** gathering evidence from outputs, logs, alerts and indicators **D3.1.3** forming and checking possible causes **D3.1.4** dependency tracing and before-and-after comparison **D3.1.5** separating root cause from symptom **D3.1.6** confirming or rejecting causes from consistent evidence
D4 Be able to identify and correct configuration settings related to user access, connectivity, storage and security that do not meet defined user requirements	**D4.1 Correction and retesting** **D4.1.1** locating the setting responsible for a fault or deviation **D4.1.2** correcting the setting to fix the fault **D4.1.3** retesting the changed setting **D4.1.4** checking related functionality (checking nothing else has been impacted by the changes or stopped working)

Pre-Accreditation Draft

Content area E: Recording outcomes and assuring readiness

Content outcome	Content detail
E1 Demonstrate knowledge and understanding of the role of recording and documenting test findings accurately and consistently to support review, accountability and improvement decisions	**E1.1 Test documentation** **E1.1.1** requirement, test condition, expected outcome, observed outcome, result and evidence reference **E1.1.2** accurate terminology and consistent structured formats **E1.1.3** results recorded as observed **E1.1.4** traceability for review and accountability **E1.1.5** use of findings to identify patterns and support improvement decisions
E2 Demonstrate knowledge and understanding of the role of clear documentation and communication in supporting accurate, consistent and effective system preparation	**E2.1 Documentation and communication** **E2.1.1** purpose, requirements, settings, changes and results **E2.1.2** handover information, status, risks, limitations and next actions **E2.1.3** consistent terminology adapted to technical and non-technical audiences **E2.1.4** effects of clear records on repeatability and fault prevention
E3 Be able to record and compare test outcomes against requirements using accurate terminology and structured formats	**E3.1 Recording and comparison** **E3.1.1** requirement, test, expected outcome, observed outcome, result and evidence **E3.1.2** terms: pass, fail and deviation **E3.1.3** requirements met, partly met and not met **E3.1.4** structured records that support review and accountability
E4 Be able to evaluate test outcomes in relation to defined requirements to determine whether systems are ready for use or require further adjustment	**E4.1 Readiness evaluation** **E4.1.1** requirement-by-requirement comparison **E4.1.2** unresolved issues, severity and impact **E4.1.3** effects of corrections already made **E4.1.4** conclusions: ready, conditionally ready or not ready **E4.1.5** further adjustments supported by evidence

Pre-Accreditation Draft

E5 Be able to document configuration decisions clearly	**E5.1 Configuration decision records** **E5.1.1** what was configured **E5.1.2** why the setting was selected **E5.1.3** the requirement or policy it meets **E5.1.4** changes from the plan and the reason **E5.1.5** supporting evidence where appropriate
E6 Be able to communicate configuration outcomes clearly and respond to queries in line with workplace procedures	**E6.1 Communicating outcomes** **E6.1.1** configured settings and results **E6.1.2** limitations, residual issues and remaining actions **E6.1.3** language and level of detail suited to the audience **E6.1.4** responses based on documented evidence in line with workplace procedures

Pre-Accreditation Draft

Transferable skills

Students are expected to develop the following transferable skills through the learning and assessment activities for this unit:

- **Analysing** when interpreting user requirements, system information and system behaviour.
- **Decision making** when selecting configuration actions in line with defined requirements
- **Communicating** when explaining configuration outcomes clearly.

The qualification Delivery Guide suggests ways for centres to help students develop these transferable skills.

Assessment summary

The NEA for this unit consists of five tasks.

- In response to Task 1, students will interpret the user and system requirements in the scenario to produce a configuration plan. The plan will identify configuration needs, dependencies, relevant policies and safe working practices, and the scope and focus of testing.
- In response to Task 2, students will prepare and configure a physical or virtual computer system in line with their plan. They will document the configuration settings applied in a configuration log, and justify their decisions and any changes made to the plan.
- In response to Task 3, students will carry out structured tests of the configured system's functionality, performance, stability, usability, accessibility and security-related behaviours. They will gather feedback from end users and record observed and expected outcomes in a testing log.
- In response to Task 4, based on the test evidence, students will identify deviations and faults, apply structured fault-finding to determine likely causes, and correct the configuration. They will then retest the affected areas and record before-and-after evidence.
- In response to Task 5, students will evaluate the final configured system against the original scenario and requirements. They will reach a reasoned judgement on whether the system is ready for use and recommend future improvements with justification.

The assessment will take 15 hours to complete.

The NEA is set by Pearson and will be marked by centres and moderated by Pearson. A new NEA for this unit will be released each September through the secure area of our website. Students must use the assessment to provide the required evidence to achieve this unit.

A sample assessment is provided on the Pearson website.

Pre-Accreditation Draft

Marking the NEA

You will make assessment decisions for the NEA using the marking grid provided below. Before making assessment decisions, you should refer to the guidance on using the marking grid provided in the *Pearson V Levels Supplementary Specification,* available on our website. A glossary of terms used in the marking grid is provided in *Appendix 1*.

Further information on managing NEAs is provided in the *Pearson V Levels Supplementary Specification,* available on our website.

Pre-Accreditation Draft

Marking grid

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 1: Plan the solution				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** review of information from the project scenario evidenced through**:** • **partial** plan of the solution that **generally** identifies user needs • **partial** test strategy with **basic** scope and methods • **general** outline of policies and safe working practices • **partial** outline of task dependencies, compatibility issues and resources	**Competent** review of information from the project scenario evidenced through: • **adequate** plan of the solution that **mostly** identifies user needs • **adequate** test strategy with **sufficient** scope and methods • **coherent** outline of policies and safe working practices • **clear** outline of task dependencies, compatibility issues and resources	**Effective** review of information from the project scenario evidenced through: • a **developed** plan of the solution that **effectively** identifies user needs • **considered** test strategy with **focused** scope and methods • **considered** outline of policies and safe working practices • **considered** outline of task dependencies, compatibility issues and resources	**Comprehensive** review of information from the project scenario evidenced through: • an **in-depth** plan of the solution that **fully** identifies user needs • **thorough** test strategy with **in-depth** scope and methods • **sophisticated** outline of policies and safe working practices • **thorough** outline of task dependencies, compatibility issues and resources

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 2: Configure the Digital Solution				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	A **basic** system configuration through suitable practical activities. Evidenced through: • **a partial** record of the configured system that suits requirements • **simplistic** record of relevant policies and safe practices followed • **some** justification of completed configuration	A **competent** system configuration through suitable practical activities. Evidenced through: • an **appropriate** record of the configured system that suits requirements • a **sufficient** record of relevant policies and safe practices followed • an **adequate** justification of completed configuration	An **effective** system configuration through suitable practical activities. Evidenced through: • a **consistent** record of the configured system that suits requirements • a **detailed** record of relevant policies and safe practices followed • a **detailed** justification of completed configuration	An **accomplished** system configuration through suitable practical activities. Evidenced through: • a **comprehensive** record of the configured system that suits requirements • a **thorough** record of relevant policies and safe practices followed • a **thorough** justification of completed configuration

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 3: Test the system and record outcomes				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	**Basic** testing of the system configuration using appropriate testing methods Evidenced through: test log that includes **generally** well-chosen tests. tests selected show **basic** understanding of the identified requirements a **partial** comparison of outcomes against expectations and applied classification such as pass fail	**Sound** testing of the system configuration using appropriate testing methods Evidenced through: a test log that includes **soundly** well-chosen tests. a **clear** understanding of why the selected tests were chosen an **appropriate** comparison of outcomes against expectations and applied classification such as pass fail	**Logical** testing of the system configuration using appropriate testing methods Evidenced through: a test log that includes **thoughtfully** well-chosen tests a **consistent** understanding of why the selected tests were chosen an **accurate** comparison of outcomes against expectations and applied classification such as pass fail	**Thorough** testing of the system configuration using appropriate testing methods Evidenced through: a test log that includes **perceptively** well-chosen tests a **comprehensive** understanding of why the selected tests were chosen a **comprehensive** comparison of outcomes against expectations and applied classification such as pass fail

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 4: Diagnose deviations, faults and carry out corrective action				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	A **basic** review of the configuration test results, user feedback and actions required. Evidenced through: **partial** identification and diagnosis of faults found **some** corrective actions offered to faults found **simplistic** solutions and or changes to the configuration applied from user feedback **partial** retesting to ensure suitability	An **adequate** review of the configuration test results, user feedback and actions required. Evidenced through: **clear** identification and diagnosis of faults found **adequate** corrective actions offered to faults found **adequate** solutions and or changes to the configuration applied from user feedback **adequate** retesting to ensure suitability	A **considered** review of the configuration test results, user feedback and actions required. Evidenced through: **proficient** identification and diagnosis of faults found **reasoned** corrective actions offered to faults found **logical** solutions and or changes to the configuration applied from user feedback a **effective** retesting to ensure suitability	A **comprehensive** review of the configuration test results, user feedback and actions required. Evidenced through: **perceptive** identification and diagnosis of faults found **in-depth** corrective actions offered to faults found **nuanced** solutions and or changes to the configuration applied from user feedback a **thorough** retesting to ensure suitability

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 5: Conclude suitability and recommend future improvements				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	A **simplistic** review of the final configured system with an evaluation against the original scenario, functionality, usability, accessibility, performance, security and reliability of the configured computer system. Evidenced through: **partial** comparison against original scenario **general** evaluation of the overall system readiness against the stated requirements with a conclusion of suitability. **basic** recommendation for future improvement with superficial justification	A **coherent** review of the final configured system with an evaluation against the original scenario, functionality, usability, accessibility, performance, security and reliability of the configured computer system. Evidenced through: **competent** comparison against original scenario **coherent** evaluation of the overall system readiness against the stated requirements with a conclusion of suitability. **adequate** recommendation for future improvement with justification	A **developed** review of the final configured system with an evaluation against the original scenario, functionality, usability, accessibility, performance, security and reliability of the configured computer system. Evidenced through: **accurate** comparison against original scenario **logical** evaluation of the overall system readiness against the stated requirements with a conclusion of suitability. **reasoned** recommendation for future improvement with justification	A **comprehensive** review of the final configured system with an evaluation against the original scenario, functionality, usability, accessibility, performance, security and reliability of the configured computer system. Evidenced through: **thorough** comparison against original scenario **thorough** evaluation of the overall system readiness against the stated requirements with a conclusion of suitability. **perceptive** recommendation for future improvement with justification

Please refer to *Pearson V Levels Supplementary Specification* for further guidance on NEAs, including how to apply the marking grids to student evidence

Pre-Accreditation Draft

Resource requirements

For this unit, students must have access to*:*

Appropriate equipment or digital technology for creating, sharing, and saving evidence

Pre-Accreditation Draft

Unit 4: Creating Digital Solutions

Assessment type: Non-exam assessment (NEA)

Unit type: Optional

Guided learning hours: 72

Introduction

Digital solutions translate user needs into workable designs. In this unit, students define the problem and its scope, identify requirements and constraints, structure solution logic, develop interface and low-fidelity representations, and produce a proposal suitable for development. They also consider responsible design, including data protection, security, accessibility, automated and AI-enabled processes, human oversight, accountability and sustainability. No specific technology, platform or programming language is required.

Students should be given opportunities to develop their knowledge and skills in a range of contexts including different problems, user requirements, system constraints and work-related scenarios.

Pre-Accreditation Draft

Teaching content

Content Area A: Problem analysis and solutions

Content outcome	Content detail
A1 Demonstrate knowledge and understanding of the purpose of analysing user needs and requirements when designing digital solutions	A1.1 Purpose of user-needs analysis A1.1.1 identifying what users need from the digital interface A1.2.1 defining what the interface should help users achieve A1.3.1 avoiding unclear requirements and unnecessary interface features
A2 Demonstrate knowledge and understanding of approaches used to define problems, determine solution scope and identify constraints,	**A2.1 Problem definition, scope and constraints** **A2.1.1** using a brief, user stories and questions to identify interface needs **A2.1.2** distinguishing essential and desirable interface features **A2.1.3** identifying what the interface will and will not include **A2.1.4** considering available devices, software, time and resources **A2.1.5** distinguishing requested features from what users need to do **A2.1.6** identifying user needs and requirements **A2.1.7** distinguishing between essential and desirable features **A2.1.8** identifying assumptions and dependencies, **A2.1.9** recognising technical, organisational and resource constraints, **A2.1.10** distinguishing between stated requirements and underlying user needs
A3 Demonstrate knowledge and understanding of the role of requirements, assumptions and success criteria in shaping solution proposals, including validation of assumptions and their impact on solution effectiveness	**A3.1 Requirements, assumptions and success criteria** **A3.1.1** functional features and non-functional needs such as usability and accessibility **A3.1.2** checking assumptions about users, devices and interface needs **A3.1.3** setting clear success criteria for the interface **A3.1.4** recognising how incorrect assumptions affect ease of use

Pre-Accreditation Draft

Content outcome	Content detail
A4 Demonstrate knowledge and understanding of the relationship between user needs, workplace context and effective digital solution design	**A4.1 User needs and workplace context** **A4.1.1** identifying the intended users, tasks and working environment **A4.1.2** matching interface features to the tasks users must complete **A4.1.3** balancing different user needs when making design choices
A5 Be able to interpret defined user needs and requirements to inform solution design	A5.1 Interpreting needs and requirements A5.1.1 identifying interface requirements from a client brief A5.1.2 identifying reasonable user needs supported by the brief A5.1.3 recording priorities and unclear requirements for checking
A6 Be able to analyse a problem to identify inputs, outputs, constraints and success criteria	A6.1 Problem analysis A6.1.1 identifying information users enter or select, A6.1.2 identifying information, messages and results shown on screen A6.1.3 identifying limits affecting the interface design A6.1.4 setting clear criteria for whether the interface meets its purpose

Pre-Accreditation Draft

Content area B: Feasibility, systems thinking and structured problem-solving

Content outcome	Content detail
B1 Demonstrate knowledge and understanding of how digital systems, components and processes influence the feasibility and structure of proposed solutions, including trade-offs between functionality, complexity and maintainability	B1.1 Feasibility and solution structure B1.1.1 identifying the devices, software and interface elements required B1.1.2 showing how screens, controls and information connect B1.1.3 checking that the interface can be created with available tools B1.1.4 balancing interface features with simplicity and reliability
B2 Demonstrate knowledge and understanding of the contribution of structured problem-solving and logical thinking to robust solution proposals	B2.1 Structured problem-solving B2.1.1 breaking the interface into screens, tasks and features B2.1.2 focusing on the information and controls users need B2.1.3 planning the order of screens and user actions B2.1.4 checking that users can complete tasks without confusion
B3 Demonstrate knowledge and understanding of the role of analysis and planning in reducing risk during later stages of development	B3.1 Analysis, planning and risk reduction B3.1.1 identifying unclear interface requirements early B3.1.2 planning design, prototyping, feedback and testing B3.1.3 reducing unnecessary changes during interface creation
B4 Demonstrate knowledge and understanding of the role of documentation and shared understanding in enabling development decisions	B4.1 Documentation and shared understanding B4.1.1 recording interface requirements and design decisions B4.1.2 using clear labels and consistent naming across designs B4.1.3 presenting designs so others can understand and comment B4.1.4 linking each key interface feature to a user requirement
B5 Be able to produce a clear and structured solution proposal suitable for development	B5.1 Structured solution proposal B5.1.1 stating the interface purpose, intended users and key requirements B5.1.2 showing screens, navigation, controls and information displayed B5.1.3 identifying practical limits, accessibility and security needs B5.1.4 providing enough detail to create the intended interface

Pre-Accreditation Draft

Content area C: Solution logic, algorithms and development approaches

Content outcome	Content detail
C1 Demonstrate knowledge and understanding of the role of structured logic and step-by-step processes in designing digital solutions to define how inputs, processes and outputs are organised, including the relationship between logic structure and predictability of outcomes	When assessing the relationship between workplace requirements, user needs, and configuration decisions, students must draw on content from Unit 2 Securing Digital Systems section A2, which details the user authentication and access permissions, secure storage, sharing and disposal of data, and reporting and escalation of suspected security incidents. Students must also draw on content from Unit 2 section A1, which details authentication requirements, access controls, update procedures, and data protection measures used to protect digital systems and services, including the relationship between authentication strength, usablity and security risk, C1.1 Structured logic and processes C1.1.1 identifying user inputs, on-screen actions and displayed outputs C1.1.2 planning buttons, choices, repeated actions and error messages C1.1.3showing the steps from a user action to an interface response C1.1.4 using clear, consistent steps so the interface behaves as expected
C2 Apply knowledge and understanding of principles of algorithms, and structured coding approaches used to represent, sequence and control solution logic within digital designs	C2.1 Algorithms and structured coding approaches C2.1.1 using ordered steps to describe interface actions C2.1.2 applying sequence, selection and repetition where needed C2.1.3 using inputs, stored values and simple validation as needed C2.1.4 using flowcharts or simple pseudocode to show interactions C2.1.5 using clear names and labels for interface actions

Pre-Accreditation Draft

C3 Demonstrate knowledge and understanding of the purpose and characteristics of low-code and block-based development approaches, including how they support rapid prototyping, iterative design and early-stage exploration of digital solution ideas	C3.1 Low-code and block-based development C3.1.1 using drag-and-drop controls, templates and built-in functions C3.1.1 creating and changing simple interface prototypes C3.1.3 improving screens using feedback and repeated changes C3.1.4.1 recognising the benefits and limits of chosen creation tools
C4 Demonstrate knowledge and understanding of principles, concepts and approaches underpinning digital design and structured logic in low-code and block-based environments, including abstraction, decomposition, sequencing, selection and iteration, and how these support the development of reliable and maintainable digital solutions	C4.1 Design principles in low-code and block-based environments C4.1.1 breaking the interface into smaller screens and features C4.1.2 placing user actions and screen changes in a logical order C4.1.3 using choices and conditions for different user responses C4.1.4 using repeated actions where the interface requires them C4.1.5 reusing consistent controls, labels and layouts
C5 Be able to structure a proposed digital solution using logical steps and processes	C5.1 Structuring solution logic C5.1.1 mapping user actions to on-screen responses C5.1.2 using ordered actions, choices and repeats where needed C5.1.3 including checks for missing entries and clear error messages C5.1.4 checking that interface actions meet the stated requirements

Pre-Accreditation Draft

C6 Be able to use appropriate development tools, environments and structured inputs, e.g. prompts for automated and AI-enabled systems, to create, refine or represent a digital solution in line with defined requirements	When creating automated and AI-enabled solutions, students must draw on content from Unit 2 Securing Digital Systems section D5, which details the the role of automated and AI-enabled detection systems in identifying potential cyber security concerns, and the need to interpret, validate and act on outputs appropriately C6.1 Development tools, environments and structured inputs C6.1.1 choosing appropriate tools for designing and creating the interface C6.1.2 using prompts, templates or settings to create interface elements C6.1.3 improving the interface through feedback and testing C6.1.4 checking generated content and interface behaviour for errors

Pre-Accreditation Draft

Content area D: User experience, interfaces and solution representation

Content outcome	Content detail
D1 Demonstrate knowledge and understanding of principles of user experience and user interface design that support usability and accessibility, including the relationship between interface design and user behaviour	D1.1 User experience and user interface design D1.1.1 organising content clearly with simple navigation D1.1.2 using consistent controls, feedback and error messages D1.1.3 using readable text and understandable instructions D1.1.4 designing for different user needs and devices D1.1.5 using clear layouts and prompts to guide user actions
D2 Demonstrate knowledge and understanding of the purpose of low-fidelity representations in communicating solution ideas during early stages of design	D2.1 Low-fidelity representations D2.1.1 using sketches, wireframes and simple interface prototypes D2.1.2 showing screen layouts, navigation and user actions D2.1.3 collecting feedback on designs before creating the interface D2.1.4 comparing and improving alternative screen designs
D3 Demonstrate knowledge and understanding of how design decisions influence usability, accessibility and system behaviour in digital solutions	D3.1 Effects of design decisions D3.1.1 how navigation, layout and controls affect ease of use D3.1.2 how colour, contrast, text and images affect accessibility D3.1.3 how input checks and default settings affect interactions D3.1.4 how design choices may help or exclude different users
D4 Be able to design solution concepts that consider system behaviour, user interaction and accessibility	D4.1 Designing solution concepts D4.1.1 planning the screens and steps users follow D4.1.2 showing what happens after buttons, links and inputs are used D4.1.3 including accessible text, navigation and controls D4.1.4 planning helpful validation and error messages

Pre-Accreditation Draft

D5 Be able to represent solution ideas using specified technical formats (e.g. documents, presentations, spreadsheets, databases)	D5.1 Technical representation D5.1.1 choosing suitable ways to show interface designs D5.1.2 using wireframes, mock-ups and simple interaction diagrams D5.1.3 labelling screens, controls and navigation clearly D5.1.4 keeping design documents consistent and easy to follow

Pre-Accreditation Draft

Content area E: Responsible design, governance, security and automated systems

Content outcome	Content detail
E1 Demonstrate knowledge and understanding of the role of automated and AI-enabled systems in supporting solution design, including generating, refining and evaluating solution approaches, and the need to assess the suitability and limitations of outputs	E1.1 Automated and AI-enabled support for design E1.1.1 using automated or AI tools to suggest interface layouts or content E1.1.2 improving interface ideas using clear prompts and feedback E1.1.3 checking suggested designs against user requirements E1.1.4 recognising errors, bias and unsuitable generated content E1.1.5 reviewing AI suggestions before using them in an interface
E2 Demonstrate knowledge and understanding of policies and procedures relating to accessibility, data protection, security and responsible design and their influence on solution proposals: designing for accessibility and diverse user needs, protection and appropriate use of personal and sensitive information, secure authentication and access control, responsible and ethical use of automated and AI-enabled systems	E2.1 Policies, procedures and responsible design E2.1.1 applying accessibility and inclusive interface design E2.1.2 collecting and displaying only necessary personal information E2.1.3 planning secure sign-in and access to appropriate features E2.1.4 using images, text and generated content responsibly E2.1.5 showing how policies influence interface features and data use
E3 Apply knowledge and understanding of governance requirements relevant to digital solutions that use automated and AI-enabled systems	E3.1 Governance for automated and AI-enabled systems E3.1.1 identifying who approves interface content and automated features E3.1.2 checking where interface data comes from and who can access it E3.1.3 keeping simple records of automated features and changes E3.1.4 planning checks and responses when automated features fail E3.1.5 ensuring users can request human help when needed

Pre-Accreditation Draft

E4 Demonstrate knowledge and understanding of potential risks associated with automated decision-making in digital systems and their implications for users and organisations, including limitations of automated decision-making and the need for human oversight	E4.1 Automated decision-making risks E4.1.1 recognising incorrect or unfair automated interface responses E4.1.2 checking that automated outputs use suitable information E4.1.3 considering privacy, security and accessibility risks E4.1.4 making automated responses understandable to users E4.1.5 providing a way to correct errors or seek human review
E5 Demonstrate knowledge and understanding of the importance of aligning proposed solutions with workplace policies and operational constraints relating to data protection, security, accessibility and acceptable system use: protection and appropriate use of personal and sensitive information, secure authentication and access control, accessibility and the needs of diverse users, acceptable use of systems, devices and services, technical, organisational and resource constraints that affect solution feasibility and implementation	E5.1 Workplace alignment and operational constraints E5.1.1 protecting personal information entered through the interface E5.1.2 using suitable logins and permissions where required E5.1.3 making screens and controls accessible to different users E5.1.4 following workplace rules for interface content and use E5.1.5 working within available devices, software and resources
E6 Demonstrate knowledge and understanding of the implications of incorporating automated and AI-enabled processes into digital solutions	E6.1 Implications of automation and AI E6.1.1 how automated features change the user journey E6.1.2 dependence on prompts, rules, data and connected services E6.1.3 checking automated responses for accuracy and privacy E6.1.4 providing clear errors and manual alternatives if automation fails
E7 Demonstrate knowledge and understanding of the importance of oversight, accountability and transparency in digital solution design	E7.1 Oversight, accountability and transparency E7.1.1 identifying who is responsible for interface decisions E7.1.2 explaining when information or responses are automated E7.1.3 keeping records of key changes and decisions E7.1.4 providing contact, feedback or review options for users

Pre-Accreditation Draft

E8 Be able to justify design decisions in relation to user needs and requirements and governance considerations	E8.1 Justifying design decisions E8.1.1 linking screen layouts and features to user requirements E8.1.2 explaining why one interface design was chosen over another E8.1.3 considering accessibility, security and responsible use of AI E8.1.4 supporting design choices with feedback and testing evidence

Pre-Accreditation Draft

Content area F: Communication, documentation and sustainable solution design

.

Content outcome	Content detail
F1 Demonstrate knowledge and understanding of sustainability considerations in digital solution design: efficient use of resources, energy consumption and device lifecycle	F1.1 Sustainability in digital solution design F1.1.1 keeping media, file sizes and data use proportionate F1.1.2 considering energy use when choosing interface features F1.1.3 designing for suitable existing devices where possible F1.1.4 balancing efficiency with accessibility and ease of use
F2 Be able to document assumptions, decisions and constraints clearly and accurately	F2.1 Documenting assumptions, decisions and constraints F2.1.1 using clear labels and consistent interface terminology F2.1.2 separating confirmed requirements from assumptions F2.1.3 recording reasons for main screen and navigation choices F2.1.4 explaining how practical limits affect the interface
F3 Be able to communicate proposed solutions clearly to technical and non-technical audiences	F3.1 Communicating solution proposals F3.1.1 using language suitable for the intended audience F3.1.2 explaining the interface purpose, features and limitations F3.1.3 using labelled wireframes, screenshots and brief notes F3.1.4 responding clearly to feedback about interface decisions
E7 Demonstrate knowledge and understanding of the importance of oversight, accountability and transparency in digital solution design	E7.1 Oversight, accountability and transparency E7.1.1 identifying who is responsible for interface decisions E7.1.2 explaining when information or responses are automated E7.1.3 keeping records of key changes and decisions E7.1.4 providing contact, feedback or review options for users

Pre-Accreditation Draft

Transferable skills

Students are expected to develop the following transferable skills through the learning and assessment activities for this unit:

- **Analysing** when interpreting user requirements, system information and system behaviour and examining user needs, system requirements and constraints to structure solutions.
- **Planning** when identifying steps, sequencing activities and considering constraints when designing a digital solution.
- **Communicating** when explaining solution proposals and explaining design decisions clearly to technical and non-technical audiences.

The qualification Delivery Guide suggests ways for centres to help students develop these transferable skills.

Assessment summary

The NEA for this unit consists of five tasks.

- In response to Task 1, students will analyse the vocational scenario to identify user needs, including secure data, inputs and outputs of a process, judge data governance problems and identify and plan their approach to designing and building a task-dependant solution.Then produce a justified assessment and scope a solution. This assessment guides the later tasks.
- In response to Task 2a, students will use their Task 1 findings to design their solution in two parts:Algorithms, using AI
- For Task 2b, UI and UX design: without using AI, students will produce screen designs, wireframes or annotated sketches that show the complete user journey and navigation, apply responsible UX and UI principles, consider accessibility and usability for different users, and explain how design decisions meet user requirements.
- In response to Task 3, students will use their plans and designs to build a prototype using low-code, no-code or block-based tool approaches. Using configurable software, templates or automation tools not hard-coding. The prototype puts planned requirements, features and interface designs in place so users can complete the main tasks. They will test and refine a prototype as they go and log key choices and improvements. The focus is on producing and improving a working solution, not on traditional programming skills.
- In response to Task 4, students will present their solution to two audiences from the scenario: one technical and one non-technical. For each audience, they will:show the main features, how end users will interact with the solution, explain how well it meets the requirements and success criteria, including limitations.

Pre-Accreditation Draft

They will also use suitable visual evidence, presented in a way that suits the audience.

- In response to Task 5, students will evaluate how suitable their solution is. They will review their design and development decisions, judge the solution against requirements, use earlier generated evidence, identify strengths, limitations and risks that could affect how the solution works in practice, and consider solution maintenance and improvements.

The assessment will take 15 hours to complete.

The NEA is set by Pearson and will be marked by centres and moderated by Pearson. A new NEA for this unit will be released each September through the secure area of our website. Students must use the assessment to provide the required evidence to achieve this unit.

A sample assessment is provided on the Pearson website.

Marking the NEA

You will make assessment decisions for the NEA using the marking grid provided below. Before making assessment decisions, you should refer to the guidance on using the marking grid provided in the *Pearson V Levels Supplementary Specification,* available on our website. A glossary of terms used in the marking grid is provided in *Appendix 1*.

Further information on managing NEAs is provided in the *Pearson V Levels Supplementary Specification,* available on our website.

Pre-Accreditation Draft

Marking grid

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 1: Plan the solution				
0 marks	1 – 3 marks	**4** – 6 marks	7 – 9 marks	10 – 12 marks
No rewardable material	Limited application of knowledge and understanding when planning a digital solution. Evidenced through: an emerging digital solution, identifying few of the requirements. a basic consideration of the problem and scope, identifying few relevant users, inputs, outputs, constraints, assumptions or success criteria, usability and accessibility will be superficial. • A superficial solution, showing a basic sequence of steps with limited consideration of decisions or outcomes.	Adequate application of knowledge and understanding when planning a digital solution. Evidenced through: a sound digital solution, identifying some of the requirements. a coherent account of the problem and scope, identifying some relevant users, inputs, outputs, constraints, assumptions and success criteria with some usability and accessibility being considered. • a competent solution, showing a generally appropriate sequence of steps and some decisions or outcomes.	Effective application of knowledge and understanding when planning a digital solution. Evidenced through: a clear digital solution, addressing most of the requirements. a focused consideration of the problem and scope, identifying most relevant users, inputs, outputs, constraints, assumptions and success criteria with usability and accessibility is mostly applied. • an effective solution, showing a logical sequence of steps, including relevant decisions and outcomes.	Comprehensive application of knowledge and understanding when planning a digital solution. Evidenced through: a thorough digital solution, addressing the requirements of the scenario. An in-depth consideration of the problem and scope, clearly defining relevant users, inputs, outputs, constraints, assumptions and success criteria with usability and accessibility full considered. • A sophisticated solution, showing a clear and coherent sequence of steps, decisions and outcomes that reflects the planned solution.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 2: Design the user experience				
0 marks	1 – 3 marks	**4** – 6 marks	7 – 9 marks	10 – 12 marks
No rewardable material	Limited application of knowledge and understanding when designing the user experience. Evidenced through: a basic design of user interaction and interface, showing few relevant screens, controls or navigation features. superficial consideration of accessible features, usability and consistent design. inconsistent use of algorithms showing a simple sequence of steps with limited consideration of decisions, inputs or outcomes.	Adequate application of knowledge and understanding when designing the user experience. Evidenced through: a sufficient design of user interaction and interface, showing some relevant screens, controls and navigation features. sufficient consideration of accessible features, usability and consistent design. appropriate use of algorithms, showing appropriate sequences and some decision-making to support the main requirements of the solution.	Effective application of knowledge and understanding when designing the user experience. Evidenced through: an effective design of user interaction and interface, showing clear screens, controls and navigation. A secure consideration of accessible features, usability and consistent design. • effective use of algorithms, showing logical sequences, decisions and alternative outcomes that support most of the solution requirements.	Comprehensive application of knowledge and understanding when designing the user experience. Evidenced through: an in-depth design showing coherent screens, interactions and navigation that meet user needs. thorough consideration of accessible features, usability and consistent design. • sophisticated use of algorithms, showing coherent sequences, decisions, validation and alternative outcomes that support the requirements of the solution.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 3: Develop the digital solution				
0 marks	1 – 3 marks	**4** – 6 marks	7 – 9 marks	10 – 12 marks
No rewardable material	Limited application of knowledge and understanding when planning a digital solution. Evidenced through: an emerging digital solution, identifying few of the requirements. a basic consideration of the problem and scope, identifying few relevant users, inputs, outputs, constraints, assumptions or success criteria, usability and accessibility will be superficial. A superficial solution, showing a basic sequence of steps with limited consideration of decisions or outcomes.	Adequate application of knowledge and understanding when planning a digital solution Evidenced through: a sound digital solution, identifying some of the requirements. a coherent account of the problem and scope, identifying some relevant users, inputs, outputs, constraints, assumptions and success criteria with some usability and accessibility being considered. a competent solution, showing a generally appropriate sequence of steps and some decisions or outcomes.	Effective application of knowledge and understanding when planning a digital solution Evidenced through: • a clear digital solution, addressing most of the requirements. • a focused consideration of the problem and scope, identifying most relevant users, inputs, outputs, constraints, assumptions and success criteria with usability and accessibility is mostly applied. • an effective solution, showing a logical sequence of steps, including relevant decisions and outcomes.	Comprehensive application of knowledge and understanding when planning a digital solution Evidenced through: a thorough digital solution, addressing the requirements of the scenario. An in-depth consideration of the problem and scope, clearly defining relevant users, inputs, outputs, constraints, assumptions and success criteria with usability and accessibility full considered. A sophisticated solution, showing a clear and coherent sequence of steps, decisions and outcomes that reflects the planned solution.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 4: Communicate your solution to technical and non-technical audiences.				
0 marks	**1 – 3 marks**	**4 – 6 marks**	**7 – 9 marks**	**10 – 12 marks**
No rewardable material	Limited application of knowledge and understanding when communicating the solution to one audience, either technical or non-technical Evidenced through: a superficial explanation of how the solution operates. a limited consideration of how far the solution meets the identified requirements. • superficial communication of limitations, with little adaptation for technical and non-technical audiences.	Adequate application of knowledge and understanding when communicating the solution to two target audiences (technical and non-technical).Evidenced through: a partially detailed explanation of how the solution operates. some consideration of how far the solution meets the identified requirements. • partially appropriate communication of limitations, with some adaptation for technical and non-technical audiences	Good application of knowledge and understanding when communicating the solution to two target audiences (technical and non-technical). Evidenced through: a mostly detailed explanation of how the solution operates. clear consideration of how far the solution meets the identified requirements. • mostly appropriate communication of limitations, adapted appropriately for technical and non-technical audiences.	Comprehensive application of knowledge and understanding when communicating the solution to two target audiences (technical and non-technical). Evidenced through: an in depth explanation of how the solution operates. thorough consideration of how far the solution meets the identified requirements. • fully appropriate communication of limitations, clearly adapted for technical and non-technical audiences.

Pre-Accreditation Draft

Mark Band 0	Mark Band 1	Mark Band 2	Mark Band 3	Mark Band 4
Task 5: Conclude suitability and recommend future improvements.				
0 marks	1 – 3 marks	**4** – 6 marks	7 – 9 marks	10 – 12 marks
No rewardable material	Limited evaluation of the suitability of the digital solution and potential improvements. Evidenced through: • a superficial justification of design and development decisions against the requirements. • a limited conclusion about the suitability of the solution against success criteria and evidence. • basic recommendations for improvement, with limited reference to identified limitations or risks.	Adequate evaluation of the suitability of the digital solution and potential improvements. Evidenced through: partially appropriate justification of design and development decisions against the requirements. a mostly supported conclusion about the suitability of the solution against success criteria and evidence. • sufficient recommendations addressing some identified limitations, risks or further development.	Good evaluation of the suitability of the digital solution and potential improvements. Evidenced through: mostly appropriate justification of design and development decisions against the requirements. a supported conclusion about the suitability of the solution against success criteria and evidence. • appropriate and prioritised recommendations addressing identified limitations, risks and further development.	Comprehensive evaluation of the suitability of the digital solution and potential improvements. Evidenced through: appropriate justification of design and development decisions against the requirements. a well-supported conclusion about the suitability of the solution against success criteria and evidence. • appropriate, prioritised and justified recommendations addressing limitations, risks and further development.

Please refer to *Pearson V Levels Supplementary Specification* for further guidance on NEAs, including how to apply the marking grids to student evidence

Pre-Accreditation Draft

Resource requirements

Students must have the following equipment for the assessment for this unit:

- Appropriate equipment or digital technology for creating, sharing, and saving evidence
- Access to an AI Agent

Final Draft V2

Unit 5: Understanding Digital Systems

Assessment type: Examined assessment

Unit type: Mandatory

Guided learning hours: 144

Introduction

Every organisation depends on digital systems, reliable data and people who understand how to use them securely and responsibly. In this unit, students explore how systems function, how data supports decision-making, how cyber security risks are managed and how digital solutions meet user needs. Realistic organisational scenarios connect these principles to everyday workplace decisions.

Students examine system components, operating systems, access control, configuration and fault diagnosis. They explore data structures, formats, quality, validation and analysis, considering how uncertainty, bias and governance affect conclusions and how visual communication supports understanding. Cyber security topics include authentication, least privilege, threats, vulnerabilities and monitoring, alongside the limitations of automated and AI-enabled detection. Problem solving and solution design cover abstraction, decomposition, algorithms, accessibility, ethics, intellectual property and sustainability.

This mandatory unit provides the conceptual foundation for the qualification and complements the practical non-exam assessment units. The examination requires students to apply knowledge to unfamiliar scenarios, interpret system information and data, and make balanced, evidence-based judgements about systems, security, data and solution design.

Students develop critical, analytical and logical thinking, problem solving, decision-making, professional judgement and clear communication. These transferable skills support progression to higher education in computing, information technology, data science and related subjects, or to higher and degree apprenticeships.
The unit also provides a foundation for employment in IT support, network and systems administration, data analysis and security operations.

Pre-Accreditation Draft

Teaching content

Content area A: Digital systems creation, configuration and fault finding

Content outcome	Content detail
A1 Understand the physical components of a digital system and their roles within the overall system structure	Students will need to know the purposes, use and characteristics of a range of hardware types. **A1.1 Processing components** **A1.1.1 Central Processing Unit (CPU)** o Control Unit (CU), Arithmetic Logic Unit (ALU), Registers, Cache, Clock speed and processor cores, Role in executing instructions and processing data **A1.1.2 Graphics Processing Unit (GPU)** o Integrated and dedicated GPUs, Role in graphics processing, visualisation and parallel processing **A1.2.3 Motherboard** o Role in connecting and allowing communication between system components, Expansion slots, buses and ports **A1.2 Memory** **A1.2.1 Random Access Memory (RAM)** o Temporary storage of programs and data currently being used, Impact of RAM capacity on system performance **A1.2.2 Read-Only Memory (ROM)** o Permanent storage of firmware and boot instructions **A1.3 Input devices** • A1.3.1 Keyboard, Mouse, Touchscreen, Microphone, Webcam, Scanner, Barcode/ QR code reader, Biometric devices, Sensors **A1.4 Output devices** • Monitor/display, Printer, Speakers/headphones, Projector, Haptic/feedback devices, Actuators in embedded and automated systems, **A1.5 Storage hardware**

Pre-Accreditation Draft

Content outcome	Content detail
	• Hard Disk Drive (HDD), Solid State Drive (SSD), USB flash storage, Memory cards, Network Attached Storage (NAS) **A1.6 Connectivity hardware** • Network Interface Card (NIC), Wireless network adapter, Bluetooth adapter, Modem, Router, Switch, Wireless access point **A1.7 Hardware interfaces and ports** • USB, HDMI, DisplayPort, Ethernet, Audio ports, Bluetooth, Wi-Fi, Role of ports and interfaces in connecting peripherals and other systems **A1.8 Network Infrastructure** **A1.8.1 Network hardware** **A1.8.1.1 Routers** o Connect different networks, Forward packets between networks, Use of IP addresses and routing information **A1.8.1.2 Network switches** o Connect devices within a local network, Forward data to the appropriate device **A1.8.1.3 Wireless access points** o Provide wireless connectivity to network devices **A1.8.1.4 Modems** o Enable communication between a local network and an internet service **A1.8.1.5 Network Interface Cards (NICs)** o Provide wired or wireless network connectivity **A1.8.1.6 Firewalls** o Control and filter network traffic, Protect systems from unauthorised access **A1.8.2 Network connections** • Ethernet, Fibre optic, Wi-Fi, Bluetooth, Mobile networks, Internet connections, • Benefits and drawbacks of using different connections in different scenarios **A1.8.3 Network structures**

Pre-Accreditation Draft

Content outcome	Content detail
	• Local Area Network (LAN), Wide Area Network (WAN), Personal Area Network (PAN), Client-server networks, Peer-to-peer networks, Cloud-based infrastructure, Benefits and drawbacks of each network structure in different scenarios **A1.8.4 Network communication** • IP addresses, MAC addresses, Data packets • Protocols: ▪ DNS, DHCP, TCP/IP, HTTP/HTTPS, ▪ The process of each protocol within network communication • Network addressing and communication between devices **A1.8.5 Network performance** • Bandwidth, Latency, Jitter, Packet loss, Throughput • Factors affecting network performance and reliability **A1.9 Data Storage** **A1.9.1 Primary storage** • RAM, Cache, Role in temporarily holding data, role in instructions being processed, Volatile nature of primary memory **A1.9.2 Secondary storage** • HDD, SSD, USB flash drives, Memory cards, o Differences in: Capacity, Speed, Cost, Reliability, Portability, Durability **A1.9.3 Network and cloud storage** • Network Attached Storage (NAS), File servers, Cloud storage, Online databases, Advantages and disadvantages of local versus cloud storage **A1.10 User Interfaces** **A1.10.1 Graphical User Interface (GUI)** • Windows, Icons, Menus, Pointer, Buttons, Forms, Dialogues, Visual feedback **A1.10.2 Command Line Interface (CLI)**

Pre-Accreditation Draft

Content outcome	Content detail
	• Text-based commands, Role of commands and parameters, Advantages for technical users and system administration, Limitations for inexperienced users **A1.10.3 Touch and gesture interfaces** • Touchscreens, Multi-touch, Gestures, Swipe, pinch and tap interactions, Use in smartphones, tablets, kiosks and other systems **A1.10.4 Voice interfaces** • Voice commands, Speech recognition, Voice assistants, Accessibility , Applications, Limitations such as background noise and recognition accuracy **A1.10.5 Natural language interfaces** • Interaction using everyday language, Chatbots and conversational systems, AI-based interfaces, Benefits and limitations **A1.10.6 User interface design** • Consistency, Navigation, Feedback, Accessibility, Usability, Readability, Error prevention and handling, Appropriate layout and controls, Matching the interface to the target users and context
A2 Know and understand the role of operating systems in digital systems	Students will need to understand the features and use of operating systems. **A2.1 Types of operating systems** • Multitasking, Real time, Network, Mobile, Batch **A2.2 Functions of an operating system:** • Managing: hardware resources, memory, files and storage, processes and applications, input and output devices • Providing: security and user accounts, a user interface **A2.3 User Accounts** • User accounts and unique user identities, Usernames and passwords, Administrator and standard/limited user accounts, Account permissions and privileges, • User account management.

Pre-Accreditation Draft

Content outcome	Content detail
	• Creating and removing accounts, Password policies, Account lockout, Disabling inactive accounts, • Authentication methods: • Passwords/PINs, Multi-factor authentication (MFA), Biometrics, Security keys/tokens **A2.4. Access Controls** **A2.4.1 Authorisation** – determining what an authenticated user is allowed to access: • File and folder permissions, Read, write, modify and execute permissions, Application and system permissions, Role-Based Access Control (RBAC), Least privilege principle, Access control lists (ACLs), Physical and logical access controls, Network access controls, Differences between authentication and authorisation. **A2.5 Secure and Effective System Use** Understand how operating systems, accounts and access controls work together to protect systems while allowing users to perform their roles effectively. • Preventing unauthorised access. • Protecting sensitive data and system resources. • Supporting accountability and auditing. • Reducing the impact of compromised accounts. • Balancing security with usability and accessibility. • Risks of weak passwords, excessive privileges, shared accounts and poor account management. • Consequences of incorrect access permissions or misconfigured security settings. • Applying appropriate security controls based on user roles and system requirements.

Pre-Accreditation Draft

Content outcome	Content detail
A3 Understand the features and use of software within digital systems	Students will need to understand the features and use of application and utility software. **A3.1 Utility software** • Antivirus/endpoint protection, Backup software, Disk management tools, File compression tools, System monitoring tools, Encryption tools, System maintenance and diagnostic tools **A3.2 Application software** • Word processing, Spreadsheets, Database software, Presentation software, Web browsers, Communication and collaboration software, Media editing software, Bespoke/custom-developed applications, Mobile applications
A4 Understand the settings required to configure a digital system	Students will need to understand the need and use of configuration settings in a digital system. **A4.1 Configuration Requirements** Understand the settings required to configure a digital system to operate correctly and meet organisational or user requirements. • Configuration profiles and system policies. • User-specific versus system-wide configuration. • Default settings and customised settings. • Hardware and software configuration requirements. • Configuration documentation and baselines. • Configuration changes and change control. **A4.2 User Account Configuration**

Pre-Accreditation Draft

Content outcome	Content detail
	• Account types and account-specific settings. • Profile settings and user preferences. • Account expiry and session settings. • Password complexity, expiry and history requirements. • Login restrictions, such as permitted devices or login times. • Group membership and inherited settings. • Configuration of user profiles across multiple devices. **A4.2 Access Permission Configuration** • Assignment of permissions to users and groups. • Inheritance of permissions from parent folders or resources. • Conflicting or overlapping permissions. • Default versus explicitly assigned permissions. • Configuration of shared-resource access. • Effects of incorrect permissions on system functionality and data access. **A4.3. Connectivity Configuration** Understand the settings required for devices to communicate successfully with networks and services. • Network adapter configuration. • IP addressing and subnet configuration. • Default gateway settings. • DNS configuration. • Proxy settings. • Wireless network configuration, including SSID and connection profiles. • VPN configuration. • Network service dependencies.

Pre-Accreditation Draft

Content outcome	Content detail
	A4.4 Storage Configuration Understand the settings that determine how data is stored. • Storage allocation and partitioning. • Drive and volume configuration. • File-system selection and configuration. • Storage quotas and user limits. • Default save locations. • Configuration of shared and network storage. • Storage capacity thresholds and their impact on system operation. • Configuration of automated storage and backup processes. **A4.5 Security Configuration** Understand the settings that determine how a system protects itself and its data. • Security policies and configuration baselines. • Firewall rules and network security settings. • Encryption settings. • Malware protection configuration. • Automatic update settings. • Screen-lock and session timeout settings. • Security logging and auditing configuration. • Configuration of security alerts and notifications.
A5 Understand the relationship between workplace requirements, user needs and system configuration as well as the risks involved	When assessing the relationship Students will need to understand the difference between workplace requirements and user needs when configurating a digital system.

Pre-Accreditation Draft

Content outcome	Content detail
	A5.1 Workplace Requirements • Organisational objectives and operational priorities. • Legal, regulatory and industry requirements. • Requirements for availability, reliability and response times. • Budget and resource constraints. **A5.2 User Needs** • User roles, tasks and technical ability. • Accessibility requirements. • Preferences for how systems are accessed and used. • Different requirements for different user groups. **A5.3 Configuration Decisions** • Selecting settings and system features to meet identified requirements. • Balancing functionality against cost and resource use. • Choosing configurations appropriate to the intended environment. • Impact of configuration choices on other system requirements. **A5.4 System Performance** • Effect of configuration choices on processing speed and responsiveness. • Resource utilisation, including CPU, memory and storage. • Optimising systems for specific workloads. • Trade-offs between performance and other requirements. **A5.5 Usability** • Ease of learning and use. • Accessibility and user efficiency. • Reducing unnecessary complexity.

Pre-Accreditation Draft

Content outcome	Content detail
	• Relationship between usability and user productivity. **A5.6 Security** • Balancing protection with ease of access. • Impact of security measures on system performance and usability. • Selecting security settings appropriate to the sensitivity of data and system use. • Consequences of prioritising convenience over security, or security over usability. **A5.7 Risks** • Misconfigured access permissions – inappropriate access may expose or allow unauthorised modification of resources. • Weak authentication settings – increase the likelihood of accounts being compromised. • Unpatched software – known security weaknesses may remain exploitable. • Exposed network services – unnecessary or publicly accessible services can provide attack opportunities. • Insecure default configurations – default passwords, settings or services may leave systems unnecessarily vulnerable. • Potential impacts – unauthorised access, data loss, service disruption, malware infection, financial loss and reputational damage.
A6 Demonstrate knowledge and understanding of technical fault diagnose, systems behaviour and resolution	Students will need to diagnose technical faults and suggest resolutions. **A6.1 System faults** • Hardware faults – component failure, damage, overheating or connection problems. • Software faults – bugs, incompatibility, corrupted files or incorrect installation. • Network faults – connection failure, configuration errors, congestion or damaged infrastructure.

Pre-Accreditation Draft

Content outcome	Content detail
	• User-related faults – incorrect operation, inappropriate settings or input errors. **A6.2 System behaviour** • Expected vs actual behaviour – identifying differences between what a system should do and what it actually does. **A6.3 Fault diagnosis and resolution** • Structured diagnosis – systematic steps to identify, isolate and resolve faults. • Diagnostic tools – logs, event viewers, monitoring tools, hardware diagnostics and network testing utilities. • System information – specifications, configuration details, error messages and status information. • Logical processes – forming, testing and eliminating possible causes. • Decision making and escalation – determining when to apply a fix, seek specialist support or escalate a fault. • Restoration and verification – confirming that functionality has been successfully restored. • Consequences of poor diagnosis or delay – increased downtime, data loss, further damage, increased costs and disruption to users.
A7 Understand how testing evidence is used to decide whether a system is fit for purpose	Students will need to understand and apply testing to digital systems. **A7.1 System Readiness, Testing and Performance** • Requirements and testing – using defined requirements to determine what should be tested and whether results are acceptable. • Test outcomes – comparing actual results against expected results and acceptance criteria. • Performance thresholds – defined limits for response time, capacity, reliability or availability.

Pre-Accreditation Draft

Content outcome	Content detail
	• Readiness decisions – deciding whether a system is ready for deployment, requires further work or should remain in its current state. • Ongoing suitability – using performance results and user feedback to determine whether a system remains fit for purpose. • Performance trade-offs – considering the effect of performance improvements on usability and security, and vice versa.

Pre-Accreditation Draft

Content area B: Responsible practice, communication and ways of working with digital systems

Content outcome	Content detail
B1 Demonstrate knowledge and understanding of the importance of safe, secure and responsible fault resolution	Students will need to understand how to carry out fault resolution responsibly **B1.1 Safe, Secure and Responsible Fault Resolution** **B1.1.1** Protecting information – prevent exposure, alteration or loss of personal and **B1.1.2** sensitive data during fault diagnosis. **B1.1.3** Confidentiality and privacy – only access information necessary to investigate the fault and protect user privacy. **B1.1.4** System integrity – avoid changes that could corrupt data, introduce vulnerabilities or affect reliable operation. **B1.1.5** System availability – minimise disruption and avoid unnecessary downtime when carrying out repairs. **B1.1.6** Legal and ethical responsibilities – follow relevant laws, organisational policies and professional codes of conduct. **B1.1.7** Controlled actions – obtain appropriate authorisation and consider the risks before making changes. **B1.1.8** Impact on others – consider how diagnostic or repair actions may affect users, services, productivity and the organisation. **B1.1.9** Secure disposal and handling – appropriately protect or dispose of data, credentials and equipment encountered during fault resolution.

Pre-Accreditation Draft

B2 Know and understand the use of Artificial Intelligence (AI) and automated decision making	When assessing the use of automated and AI-enabled solutions, students should draw on content from Unit 2 Securing Digital Systems section D6, relating to the limitations of responses created by automated and AI-enabled system Students will need to understand how AI in used in decision making within organisations **B2.1 Automated decision-making** • use of rules, algorithms and data to make or support decisions. **B2.2 AI-enabled decisions** • use of AI to analyse data, identify patterns and provide predictions or recommendations. **B2.3 Limitations** • effects of inaccurate, incomplete or biased data, unreliable outputs and situations outside the system's capabilities. **B2.4 Bias** • how data, algorithms and system design can introduce or reinforce unfair outcomes. **B2.5 Human oversight** • importance of reviewing, questioning and, where appropriate, overriding automated or AI-generated decisions. **B2.6 Implications** • potential effects on individuals, organisations, fairness, trust and decision-making.

Pre-Accreditation Draft

B3 Know and understand the use of AI prompts, outputs and their implications	Students will need to understand and be able to use AI prompts, the outputs they can generate and the implications of using AI **B3.1 Prompts and structured inputs** • how instructions, questions, data and input formats are used to generate outputs. **B3.2 Prompt design** • how clarity, specificity, context and structure influence the relevance and quality of generated outputs. **B3.4 Input and output relationships** • how changes to prompts or input data can affect the resulting output. **B3.5 Social implications** • impacts of automated and AI-generated outputs on individuals, organisations, employment, access to information and society. **B3.6 Ethical implications** • issues relating to fairness, bias, privacy, transparency, accountability and responsible use.

Pre-Accreditation Draft

B4 Know and understand the need for communication in technical support	Students will need to understand the importance of good communication in technical support **B4.1 Information gathering and interpretation** • obtaining, clarifying and analysing information to support accurate identification of issues. **B4.2 Clear and accurate communication** • conveying consistent, reliable information using appropriate technical or non-technical language. **B4.3 Communication approaches** • selecting appropriate verbal, written and digital methods to support clarity, efficiency and effective service delivery. **B4.4 Adapting communication** • adjusting language, level of detail, tone and communication methods to meet different audience and user needs. **B4.5 Confidentiality and privacy** • protecting personal, sensitive and technical information when communicating or sharing support information. **B4.6 User queries and expectations** • responding appropriately, managing expectations and communicating support actions, timescales and outcomes. **B4.7 Professional and ethical practice** • communicating respectfully, responsibly and objectively in accordance with organisational requirements. **B4.8 Documentation** • recording relevant issues, actions, findings and outcomes to support ongoing technical support. **B4.9 Communication and troubleshooting**

Pre-Accreditation Draft

	• distinguishing between communication activities that support the user and technical activities involved in diagnosing and resolving issues.

Content area C: Principles of problem solving, programming logic and digital solution design

Content outcome	Content detail
C1 Know and understand how to solve problems	Students will need to demonstrate an understanding of how these principles work together as a structured problem-solving process. **C1.1 Principles of computational problem solving** **C1.1.1** Understanding a problem and identifying the required outcome **C1.1.2** Identifying inputs, processes and outputsc **C1.1.3** Identifying constraints, requirements and assumptions **C1.1.4** Breaking complex problems into manageable parts **C1.1.5** Identifying patterns and relationships within problems **C1.1.6** Developing logical and systematic approaches to problem solving **C1.1.7** Evaluating alternative solutions and selecting an appropriate approach **C1.2 Abstraction** **C1.2.1** Removing unnecessary detail from a problem **C1.2.2**Identifying the important features, data and processes required to solve a problem **C1.2.3** Representing complex systems using simplified models **C1.2.4** Identifying common features and generalising solutions **C1.2.5** Using abstraction to make problems easier to understand and solve

Pre-Accreditation Draft

	C1.2.6 Understanding the advantages and limitations of abstraction **C1.3 Decomposition** **C1.2.1** Breaking a complex problem into smaller, manageable sub-problems **C1.2.2** Identifying the tasks and processes required to solve a problem **C1.2.3** Developing modular solutions **C1.2.4** Dividing a solution into functions, procedures, modules or components **C1.2.5** Solving and testing individual components before integrating them **C1.2.6** Understanding how decomposition improves maintainability, testing and debugging
C2 Know and understand how to collaborate when developing digital solutions	Students will need to understand the collaboration process when developing digital solutions **C2.1 Roles and responsibilities** • how different roles, perspectives and areas of expertise contribute to solution development and decision making. **C2.2 Collaborative decision-making** • sharing ideas, evaluating options and reaching informed decisions collectively. **C2.3 Constraints and priorities** • how technical, organisational, financial, time and resource constraints influence decisions and solution design. **C2.4 Structured collaboration** • use of defined roles, task allocation, agreed processes, meetings and shared documentation to coordinate development. **C2.5 Inclusive collaboration** • ensuring different perspectives, abilities and user needs are considered when developing solutions. **C2.6 Responsible collaboration**

Pre-Accreditation Draft

	• acting ethically, respecting others' contributions and considering the potential impact of decisions. **C2.7 Quality and consistency** • how effective collaborative working can improve solution quality, reduce errors and support consistent outcomes. **C2.8 Managing challenges** • addressing conflicting opinions, priorities, communication issues and competing requirements.
C3 Know and understand the relationship between user needs, feedback and refinement	Students will need to know how user needs are identified, interpreted and translated into digital solution design through feedback and refinements. **C3.1 Identifying user needs** • gathering information about user requirements, tasks, preferences and expectations. **C3.2 Interpreting requirements** • analysing user information to identify priorities and translate needs into design requirements. **C3.3 Translating needs into designs** • using user requirements to inform features, functionality, interfaces and solution design. **C3.4 Shared understanding** • ensuring users and development teams have a common understanding of requirements and proposed solutions. **C3.5 Feedback** • gathering and evaluating feedback from users and stakeholders to identify improvements. **C3.6 Iteration and refinement**

Pre-Accreditation Draft

	• modifying and retesting designs in response to feedback and changing requirements. **C3.7 User-focused outcomes** • evaluating whether the final solution meets identified user needs and requirements.
C4 Understand and be able to apply programming logic to solve problems	Students will need to use logic and processes of digital systems to solve problems and communicate solutions. **C4.1 Logical thinking and programming fundamentals** • Using logical thinking to determine how a digital solution should operate • Identifying relationships between inputs, processes and outputs • Applying logical operators such as AND, OR and NOT • Using Boolean values • Developing conditions and logical tests • Using comparison and arithmetic operators when creating rules and calculations • Tracing the flow of a solution to identify expected outcomes • Applying logical thinking when configuring automated processes and workflows **C4.2 Sequencing** • Understanding the importance of the order in which instructions are executed • Identifying sequential processes within an algorithm • Determining dependencies between actions, components and processes • Developing algorithms using logically ordered actions • Understanding the consequences of incorrect sequencing

Pre-Accreditation Draft

	• Tracing sequential algorithms to predict outputs **C4.3 Selection** • Using decision-making within algorithms and programs • IF, IF/ELSE and nested IF structures • Using multiple conditions to determine different outcomes • Selecting appropriate conditions and comparison operators • Configuring different actions depending on user input, data values or system conditions • Testing different branches of a selection structure • Understanding how selection allows a solution to respond differently to different inputs **C4.4 Iteration** • Understanding the need to repeat instructions or processes • Using repetition features provided by low code/no code platforms • Count-controlled iteration such as FOR loops • Condition-controlled iteration such as WHILE and REPEAT/UNTIL loops • Selecting an appropriate iteration structure for a specific requirement • Avoiding infinite loops • Testing loops using normal, boundary and invalid data • Tracing iterations to determine outputs and identify errors **C4.5 Algorithm design and representation** • Developing step-by-step algorithms to solve problems • Using flowcharts to represent processes and logic • Using structured English to describe solutions

Pre-Accreditation Draft

	C4.6 Structured approaches to digital solution design • Analysing requirements before developing a solution • Identifying functional and non-functional requirements • Developing a solution specification • Designing inputs, processes, outputs and user interactions • Identifying data requirements and appropriate data structures • Selecting appropriate low code, no code development tools • Producing design documentation before implementation **C4.7 Development of digital solutions** • Building digital solutions using low-code, no-code and visual development environments • Configuring components, controls, forms, data sources and workflows • Creating rules, formulas, conditions and automated processes • Developing solutions incrementally and refining them as requirements are addressed • Creating and testing individual components or workflows • Integrating components, data sources and automated processes into a complete solution • Reusing existing components, templates and pre-built functionality where appropriate • Configuring permissions, validation and error-handling features • Testing the behaviour of workflows, rules and components • Identifying and resolving configuration, logic, data and runtime problems

Pre-Accreditation Draft

	• Using platform features such as version history, testing environments and deployment controls to manage changes • Evaluating the completed solution against its original requirements • Understanding the limitations of low-code/no-code development and identifying when alternative development approaches may be required **C4.8 Testing digital solutions** • Developing a structured test strategy for a low-code/no-code digital solution • Creating test plans, test scenarios and test cases • Testing individual components, workflows, rules, forms and the complete solution • Testing data inputs, calculations, validations and automated processes • Using normal, boundary, invalid and extreme test data • Testing expected and unexpected user behaviour • Testing different decision branches and workflow paths • Testing automated processes and actions triggered by different conditions • Testing interactions between components, data sources, workflows and external services • Testing user interfaces, navigation and data entry • Recording expected and actual results • Identifying errors, failures and unexpected behaviour • Distinguishing between configuration, data, logic, integration and runtime errors • Using platform testing features, previews, logs and other available diagnostic information

Pre-Accreditation Draft

	• Testing that permissions, validation and security controls operate as intended • Using test results to determine whether the solution meets its requirements • Repeating tests after changes have been made to confirm that the solution continues to operate correctly **C4.9 Debugging and refinement** • Identifying the cause of errors and unexpected behaviour within a digital solution • Using systematic approaches to identify problems in workflows, rules, configurations, data and components • Tracing the flow of data and processes through a digital solution • Using platform features such as test runs, logs, run history, error messages and diagnostic information • Checking inputs, conditions, formulas, dependencies and outputs to identify the source of a problem • Correcting configuration or logic problems without introducing new problems • Retesting solutions after changes have been made • Refining workflows, rules, interfaces and processes to improve the solution • Improving efficiency, usability, accessibility, reliability and maintainability • Simplifying workflows and removing unnecessary processes or components • Refining user interfaces and interactions based on testing and user feedback • Improving data validation and error handling • Optimising automated processes and integrations • Evaluating the impact of changes on other components and processes

Pre-Accreditation Draft

	• Carrying out regression testing to ensure existing functionality continues to work • Evaluating whether the refined solution meets the original requirements **C4.10 Evaluation of digital solutions** • Comparing the completed solution against its original requirements and success criteria • Evaluating whether the solution effectively addresses the identified problem • Evaluating the effectiveness of workflows, rules, automation and configured functionality • Assessing performance, usability, accessibility, security, reliability and scalability • Evaluating the quality and accuracy of data used by the solution • Assessing the effectiveness of integrations with other systems or services • Considering feedback from users and stakeholders • Identifying limitations of the chosen low-code/no-code platform • Identifying limitations caused by configuration, available components, integrations or platform functionality • Identifying potential improvements to the solution • Considering whether additional custom development or alternative tools may be required • Evaluating the maintainability and future development of the solution • Making recommendations for further development based on testing, user feedback and evaluation findings

Pre-Accreditation Draft

C5 Know and understand the importance of ethical, legal and sustainable digital practice	Students will need to understand how to adhere to ethical, legal and sustainable digital practice. **C5.1 Intellectual property** • copyright, trademarks, patents and other rights protecting digital content, software and creative work. **C5.2 Ownership and attribution** • establishing ownership of digital content and giving appropriate credit when using the work of others. **C5.3 Responsible use of digital content** • respecting licensing requirements, permissions and restrictions when using or sharing digital resources. **C5.4 AI and automated systems** • responsible use of AI-generated content and outputs, including checking accuracy, bias, ownership and appropriate use. **C5.5 Ethical considerations** • fairness, transparency, accountability, privacy and the potential impact of digital technologies on individuals and society. **C5.6 Sustainability** • environmental impacts of digital technologies, including energy consumption, electronic waste, equipment lifecycle and responsible resource use. **C5.7 Legal and organisational requirements** • following relevant legislation, regulations, licences and organisational policies when using digital technologies and content.

Pre-Accreditation Draft

Transferable skills

Students are expected to develop the following transferable skills through the learning and assessment activities for this unit:

- **Communicating** in a professional manner to specialist and non-specialist audiences. Clarity and precision in the use of technical terminology.

The qualification Delivery Guide suggests ways for centres to help students develop these transferable skills.

Assessment summary

A written examination worth 110 marks. The duration of the written examination is 2 hours and 30 minutes and it must be taken under supervised conditions in the period timetabled by Pearson.

Students will be assessed through a number of short-answer and long-answer questions. The questions will assess knowledge and understanding of digital concepts and how they are used to solve problems.

Sample assessment materials will be available on our website to help centres prepare students for the assessment.

The assessment is available in May/June each academic year. The first assessment is May/June 2029.

Resource requirements

Students must have the following equipment for the assessment for this unit:

- Appropriate equipment or digital technology for creating, sharing, and saving evidence

Pre-Accreditation Draft

4 Planning your programme

Is there a student entry requirement?

There are no formal entry requirements. Students are expected to study this qualification alongside other vocational qualifications, A levels or English and/or maths qualifications. Centres are responsible for ensuring that students make reasonable progress and achieve at this level. Achievement can be supported by highlighting links between this qualification and other qualifications.

What level of sector knowledge is needed to teach this qualification?

We do not set any requirements for teachers but recommend that centres review the skills and knowledge of the teaching team to ensure they remain relevant and up to date. This will help ensure that students benefit from teaching that reflects current sector practice and from programmes that support progression.

What resources are required to deliver this qualification?

As part of your centre approval, you will need to show that the necessary resources and workspaces are available to deliver the qualification. For some units, specific resources are required; please refer to individual units.

What makes good vocational teaching?

Effective vocational teaching is rooted in the application of knowledge, understanding and skills within the sector. Teaching and learning should be contextualised through realistic vocational activities, scenarios and projects that help students connect what they learn with how the sector operates in practice. Through opportunities to apply their learning, supported by practice, feedback and reflection, students can develop their understanding and skills over time and build confidence in applying their learning in different contexts. To support this, we provide delivery guidance for the qualification and CPD to support effective delivery.

Pre-Accreditation Draft

5 Final grading and awarding

Awarding and reporting for the qualification

V Level qualifications are graded on a seven-grade scale from A* to E, and P (Pass). Students who do not meet the minimum requirements for a qualification grade will be recorded as Unclassified (U) and will not be certificated.

Individual units will be graded on the same grade scale. Individual unit results will be reported.

Grade boundaries are set for each unit in the series in which it is offered through a process known as awarding. Awarding is used to set grade boundaries and ensure that standards are maintained over time. This ensures that students have the same opportunity to achieve regardless of the assessment opportunity.

Students' unit 'raw' marks will be converted to a Uniform Mark Scale (UMS). The UMS is used to convert students' unit raw marks into uniform marks. This is done to standardise marks across assessment series. Further details of the UMS are provided below in the section 'Calculation of a Qualification Grade'.

The awarding and certification of the qualification will comply with the requirements of the Office of Qualifications and Examinations Regulation (Ofqual).

Eligibility for an award

In order to be awarded a qualification, a student must achieve an outcome for all units and achieve the minimum number of overall uniform marks at a qualification grade threshold.

There are no 'must-pass' units within the qualification. A unit result of Unclassified is considered an outcome for the purposes of aggregating a final award.

Subject to eligibility, Pearson will automatically calculate the qualification grade for your students when the qualification claim is made.

In order to meet the terminal assessment requirement, a student must take the examined assessment unit in their final series, that is, the one in which the final award is claimed. If a student retakes the examined assessment, only the result from the final attempt will be used towards thequalification grade, even if an earlier attempt achieved a higher result.

Pre-Accreditation Draft

Calculation of the qualification grade

The final qualification grade represents an aggregation of a student's performance across all units. Stronger performance in some units may be balanced by lower performance in others.

The UMS converts students' unit 'raw' marks into uniform marks. This is done to standardise marks across different assessment series. For example, a student who achieves an E in a unit one year will receive the same uniform mark as a student achieving the same grade in a later series, regardless of their raw marks.

The minimum uniform marks required for each grade for each unit

Units 1, 2 and 3 /4

Unit Grade	A*	A	B	C	D	E	P
Maximum UMS =80	72	64	56	48	40	32	24

Students who do not achieve the standard required for a P will receive a uniform mark in the range 0–23.

Unit 5

Unit Grade	A*	A	B	C	D	E	P
Maximum UMS = 160	144	128	112	96	80	64	48

Students who do not achieve the standard required for a P will receive a uniform mark in the range 0–47.

Qualification level results: the minimum uniform marks required for each grade

Qualification Grade	A*	A	B	C	D	E	P
Maximum UMS = 400	360	320	280	240	200	160	120

Students who do not achieve the standard required for a P grade will receive a uniform mark in the range 0–119.

Results issue

Results are issued in line with the published dates shown in the 'Key dates' section of the *Information Manual*, available on our website

Pre-Accreditation Draft

6 Resources and support

We provide a range of resources and professional development opportunities to support the delivery of V Levels. These are available on our website.

Support for setting up your course and preparing to teach

Delivery Guide

The Delivery Guide provides an overview of the qualification units and assessments. It includes a broad scheme of work, with guidance on delivery, teaching approaches, assessment preparation and additional resources.

Support for teaching and learning

Pearson provides a range of resources to support the teaching and learning of vocational qualifications. Details of Pearson's own resources and all endorsed support materials are available on our website.

Resources may also be available from other publishers.

Support for assessment

Sample assessment materials (SAMs) for examined assessment units

Sample assessment materials are available for the examined unit/s and can be downloaded from the Pearson Qualifications website. An additional set of materials will also be available prior to the first live assessment, allowing your students further opportunities for practice.

Sample NEAs

Sample NEAs are available for the non-exam units and can be downloaded from the Pearson Qualifications website.

Centre standardisation materials for NEA units

Marked examples of student work will be provided to support the centre marking and standardisation process.

Pre-Accreditation Draft

Training and support from Pearson

Training and professional development

We provide a range of training and professional development events to support the introduction, delivery, assessment, quality assurance and administration of V Levels. These sector-specific events are developed and delivered by subject specialists.

People to talk to

There are many people who can support you and give you advice and guidance on delivering your V Levels. They include:

- Subject Advisors – they are available for all sectors. They have expertise across Pearson qualifications within their sector and can answer queries on planning, teaching, learning and assessment.
- Customer Services – the 'Support for You' section of our website explains how to contact us for general queries. For specific queries, our service teams will direct you to the relevant person or department.
- Pearson Quality Advisors – they can support centres with the quality assurance aspects of programme delivery.

Pre-Accreditation Draft

Appendix 1

Glossary of terms used for NEA marking grids

Level-based descriptor	Generic Level 3 NEA evidence definition
Accomplished	Evidence demonstrates highly developed and well-controlled knowledge, understanding or skill, producing a polished and effective outcome.
Accurate	Evidence is correct and precise, with few or no substantive errors in the knowledge, reasoning, processes or outcomes presented.
Adequate	Evidence meets the essential requirements of the task but may lack breadth, depth, precision or consistency.
Appropriate	Evidence is relevant and suitably matched to the task, context, purpose or intended outcome.
Basic	Evidence addresses straightforward aspects of the task but shows only elementary knowledge, reasoning, control or development.
Clear	Evidence is readily understood, relevant points are expressed directly, and the relationship between ideas, actions or outcomes is apparent.
Coherent	Evidence is logically connected and forms a consistent line of reasoning, process or response.
Competent	Evidence demonstrates a sound and dependable standard of knowledge, understanding or skill sufficient to meet the task requirements.
Comprehensive	Evidence covers the relevant aspects of the task in substantial breadth and depth, with few significant omissions.
Concise	Evidence communicates the required information economically and precisely without unnecessary material.
Confident	Evidence shows secure and purposeful application, with decisions or skills carried out with limited hesitation or uncertainty.
Considered	Evidence shows that relevant information, alternatives or implications have been deliberately examined before choices or conclusions are made.

Pre-Accreditation Draft

Level-based descriptor	Generic Level 3 NEA evidence definition
Consistent	Evidence maintains an appropriate standard across the response, process or outcome, with limited variation in quality or control.
Convincing	Evidence presents well-supported reasoning or outcomes that provide a strong basis for accepting the conclusion, choice or judgement.
Critical	Evidence examines assumptions, evidence and alternatives closely rather than accepting information at face value, leading to a well-supported judgement.
Detailed	Evidence includes specific and relevant information that develops the response beyond general or outline statements.
Developed	Evidence extends ideas, reasoning or work sufficiently, showing progression and purposeful elaboration.
Effective	Evidence achieves the intended purpose or outcome and is supported by relevant, well-applied knowledge, reasoning or skill.
Emerging	Evidence shows early signs of the required knowledge, reasoning or skill, but these are not yet secure or consistently demonstrated.
Focused	Evidence remains closely directed towards the task, purpose or intended outcome and avoids significant irrelevant material.
Fluent	Evidence is produced smoothly, accurately and with sustained control, with ideas or skills integrated naturally.
Fully	Evidence demonstrates the required quality, coverage or application across all relevant aspects of the task.
Imbalanced	Evidence gives disproportionate attention to some factors or viewpoints and does not weigh relevant considerations fairly.
Inconsistent	Evidence varies noticeably in relevance, accuracy, control or quality across the response or outcome.
In-depth	Evidence explores relevant aspects with substantial detail, explanation and sustained reasoning.

Pre-Accreditation Draft

Level-based descriptor	Generic Level 3 NEA evidence definition
Insightful	Evidence demonstrates a strong and perceptive understanding of significance, relationships or implications that may not be immediately obvious.
Literal	Evidence deals mainly with explicit or surface meaning and shows little interpretation of wider significance, relationships or implications.
Logical	Evidence follows a valid and orderly sequence in which conclusions, decisions or outcomes arise from the information presented.
Mostly	Evidence demonstrates the stated quality across the greater part of the response or outcome, although some noticeable weaknesses remain.
Nuanced	Evidence recognises subtle distinctions, qualifications or competing factors and reflects these in the reasoning or judgement.
Obvious	Evidence identifies readily apparent features or choices but does not explore less immediate relationships, implications or alternatives.
Occasionally	Evidence demonstrates the stated quality at some points, but not frequently or consistently enough to characterise the response overall.
Partial	Evidence addresses only part of the task or demonstrates the required quality incompletely, with important gaps or undeveloped areas.
Perceptive	Evidence identifies and explains important meanings, relationships or implications with a high degree of discernment.
Pertinent	Evidence is directly relevant and makes a purposeful contribution to the task, reasoning or outcome.
Proficient	Evidence demonstrates well-developed, reliable and controlled knowledge, understanding or skill in completing the task.
Reasoned	Evidence uses connected reasons and relevant support to explain decisions, conclusions or judgements.
Relevant	Evidence relates appropriately to the task, context, issue or intended outcome.

Pre-Accreditation Draft

Level-based descriptor	Generic Level 3 NEA evidence definition
Reliable	Evidence demonstrates dependable reasoning, processes or outcomes that are sufficiently accurate and consistent for the intended purpose.
Secure	Evidence demonstrates firmly established knowledge, understanding or skill, applied with consistent control and few significant weaknesses.
Simplistic	Evidence reduces an issue or task to basic points and overlooks relevant complexity, relationships or competing factors.
Some	Evidence addresses a limited number of the points required by the task or content. Coverage is incomplete and uneven, but it is more than a single, isolated or token reference.
Sophisticated	Evidence demonstrates highly developed, integrated and discerning knowledge, reasoning or skill, handled with precision and subtlety.
Sound	Evidence demonstrates a generally secure and credible standard, supported by relevant knowledge, reasoning or skill, despite some limitations.
Straightforward	Evidence presents an uncomplicated and generally relevant response but shows limited complexity, depth or development.
Sufficient	Evidence provides enough relevant coverage, support or control to meet the task requirements, though it may not be extensive.
Suitable	Evidence is appropriate for a particular purpose.
Superficial	Evidence addresses surface features but lacks explanation, analysis, development or engagement with underlying significance.
Sustained	Evidence maintains the stated quality, line of reasoning or level of control across the response, process or outcome.
Thorough	Evidence addresses the relevant aspects of the task carefully and in substantial breadth and depth, with strong supporting detail and few omissions.

Pre-Accreditation Draft

Level-based descriptor	Generic Level 3 NEA evidence definition
Uneven	Evidence varies in quality or control, with stronger and weaker aspects across the response or outcome.

Pre-Accreditation Draft

Appendix 2

Command word taxonomy for examined assessment

This is a summary of the key terms that may be used in examined assessment. This is a summary of the key terms that may be used in external assessment. Please note, the list below will not necessarily be used in every paper/session and is provided for guidance only.

Command word	Simplified definition
Complete	Add the required information to a table, diagram or other given format.
Describe	Give an account of something or set out the stages of a process. Include relevant detail, but reasons or justification are not required.
Discuss	Consider different aspects of an issue, situation, problem or argument in detail and explain how they relate to each other. A conclusion is not required.
Draw/write	Create a visual or written representation of information.
Evaluate	Review relevant information and evidence, consider strengths, weaknesses or alternatives, and reach a supported judgement. Where required, make an appropriate recommendation.
Explain	Give a relevant point and a linked reason that shows why or how something occurs.
Identify	Select the required relevant information, usually from a stimulus or resource.
State/give/name	Recall and provide the required piece or pieces of information.

Pre-Accreditation Draft

Appendix 3

Mapping between Department for Education (DfE) subject content and Pearson content and Pearson Level 3 V Level in Digital Systems and Data

DfE WRP 1 Prepare, analyse, interpret and present data from different sources to support conclusions and decision making	
DfE Digital Systems and Data V Level subject content statement	**Pearson qualification**
the purpose of preparing, analysing, interpreting and presenting data to generate insights that support conclusions and decision making in workplace contexts	Unit 1: A1
how data is structured, formatted and defined within datasets from different sources, including how levels of detail affect interpretation, comparability and use	Unit 1: A2
data quality issues arising from missing data, duplicate records, inconsistent formats and conflicting values across sources and their impact on analysis	Unit 1: A5
methods used to validate and prepare data prior to analysis through checking formats and data types, confirming completeness, verifying value ranges and resolving inconsistencies	Unit 1: A6
analytical techniques used to examine prepared datasets: sorting, filtering, and grouping records; calculating totals, averages and percentages and rates of change, comparing categories and ranking results; identifying trends, patterns and anomalies; selecting techniques in relation to data type and analytical purpose, and interpreting variability and relationships within datasets	Unit 1: B1
the role of automated and AI-enabled analytical systems in supporting pattern identification and insight generation, and the need to interpret outputs critically	Unit 2: D6; Unit 4: E1; Unit 3: C5
the forms and uses of analytical outputs, including summaries, comparisons, trends and indicators, and how these inform conclusions and decision making	Unit 1: C1
how combining datasets from different sources can reveal relationships and insights not visible when sources are analysed separately, including risks associated with inconsistent definitions and alignment across sources	Unit 1: B2
the role of metadata, field definitions and documentation in supporting analysis, transparency, accountability and correct interpretation of analysed outputs	Unit 1: A2
policies and procedures relating to data privacy, confidentiality and responsible data use and presentation of insights: collection, storage and	Unit 4: E2; Unit 1: A3; Unit 2: E1

Pre-Accreditation D

retention of data; access permissions and authorised use of data; anonymisation and protection of personal or sensitive information	
the relationship between data preparation, analytical methods and the reliability of conclusions	Unit 1: B3
the relationship between data quality, analytical approach, data limitations, uncertainty and confidence in conclusions, including the impact of outliers, sampling bias and unrepresentative data	Unit 1: A5
the impact of bias, incompleteness and lack of representativeness in data on analytical outcomes and interpretation	Unit 1: A5
limitations of datasets used in automated and AI-enabled analysis and potential sources of bias in data collection, preparation, processing and when drawing conclusions	Unit 1: A4; Unit 1: C9
governance and data protection requirements relevant to the use of data in automated and AI-enabled analysis: lawful and appropriate use of data, protection of personal and sensitive information, transparency and explainability of automated outputs, accountability and human oversight, and accuracy, fairness and mitigation of bias in data and analytical processes	Unit 4: E2; Unit 4: E3
the importance of transparency when presenting insights generated and supported by automated and AI-enabled systems	Unit 4: E3
how automated visualisation tools may influence interpretation of findings, including the influence of scale, proportion and representation	Unit 1: C2
the consequences of presenting automated outputs without explaining assumptions, limitations and confidence in the underlying data and analysis	Unit 1: A4
how workplace setting, audience needs and decision-making purpose influence the selection of presentation formats	Unit 1: C3
principles of visual communication that support accurate, transparent, proportionate and non-misleading representation of analysed data findings	Unit 1: C4
the relationship between analytical findings and presentation choices and user interpretation of information	Unit 1: C5
the role of interpretation and professional judgement in transforming analytical results into meaningful conclusions, including distinguishing correlation from meaningful relationships	Unit 1: C6
principles of inclusive and unbiased data handling that support fair, accurate and responsible interpretation of analytical findings, including recognising potential bias in data collection and representation, considering completeness and representativeness of datasets, avoiding misleading comparisons or visualisations, presenting findings objectively and transparently, considering the needs of diverse users and audiences	Unit 1: D1
inclusive and accessible presentation practices that support understanding by diverse users and audiences	Unit 3: C3
sustainability considerations relating to the preparation, storage and sharing of data outputs	Unit 1: A7
interpret a defined analytical and decision-making purpose	Unit 1: C7

Pre-Accreditation Draft

examine data from different sources to determine suitability for analysis	Unit 1: A6; Unit 1: A2
prepare data for analysis through validation, checking formats and confirming completeness	Unit 1: A6
analyse prepared datasets to identify patterns, relationships and trends	Unit 1: B4
examine analytical outputs in relation to the defined purpose	Unit 1: C8
interpret analytical findings and consider potential sources of bias and limitation in the data	Unit 1: C9
draw reasoned conclusions from analysed data	Unit 1: B5
select and apply graphical and tabular visualisation formats to present analysed insights clearly and accurately	Unit 1: C10
ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations	Unit 1: C11
communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences	Unit 1: C12
document analytical decisions, assumptions and outputs clearly	Unit 1: C13
review presented outputs to improve clarity, accessibility and relevance	Unit 1: C14

DfE WRP2
Apply security protocols and interpret system information to detect and escalate cyber security concerns

DfE Digital Systems and Data V Level subject content statement	Unit in Pearson qualification
authentication requirements, access controls, update procedures and data protection measures used to protect digital systems and services, including the relationship between authentication strength, usability and security risk, and principles of least privilege	Unit 2: B1; Unit 2: A1; Unit 5: A2.3-A2.5
policies relating to acceptable use, access control, data handling and incident reporting, and their role in guiding secure practice: acceptable use of systems, devices and services, user authentication and access permissions, secure storage, sharing and disposal of data, and reporting and escalation of suspected security incidents	Unit 4: E5; Unit 3: A2; Unit 2: A2
common cyber security threats: phishing, social engineering, malware, ransomware, unauthorised access attempts, suspicious network behaviour and data loss incidents	Unit 2: A3
the use of system logs, alert notifications and account activity records to identify indicators of potential cyber security concerns, including correlation of multiple indicators and distinguishing normal system variation from anomalous behaviour	Unit 2: C1; Unit 2: D1

Pre-Accreditation Draft

the relationship between system activity, security-related information and potential cyber security concerns, including uncertainty in interpretation and the need for professional judgement	Unit 2: D1
the role of baseline system behaviour in identifying deviations and potential threats	Unit 2: D2
the relationship between security controls, user behaviour and system vulnerabilities	Unit 2: D3; Unit 5: A5.6-A5.7
the implications of different types of cyber threats and the impact of delayed identification and escalation	Unit 2: D4; Unit 5: A5.7
policies and procedures relating to privacy, confidentiality and responsible handling of security-related information: storing information securely, restricting access to authorised users, transmitting information appropriately and reporting concerns through defined procedures	Unit 2: E1
the importance of accurate interpretation of system information, awareness of false positives and misinterpretation of automated alerts, and the limitations of automated and AI-enabled detection systems	Unit 2: D5; Unit 5: B2
the role of automated and AI-enabled detection systems in identifying potential cyber security concerns, and the need to interpret, validate and act on outputs appropriately	Unit 2: D6; Unit 5: B2
energy efficiency, data retention management and secure device lifecycle practices relevant to cyber security	Unit 2: B4
authentication requirements, access controls, update procedures and data protection measures to digital systems	Unit 2: B1; Unit 2: A1; Unit 5: A2.3-A2.5
configuration actions relating to user accounts, permissions and security settings in line with defined security procedures	Unit 2: B2
apply procedures for secure access, authentication and system use	Unit 2: B3
review security-related information to identify slow response times, repeated errors, failed updates and connectivity interruptions, and what these indicate about system quality	Unit 2: C2
recognise signs of unexpected and anomalous system activity	Unit 2: C3
use log files, monitoring dashboards and system alerts to view and interpret security-related information	Unit 2: C4
record observations clearly and accurately	Unit 2: C5
escalate potential cyber security concerns in line with security procedures	Unit 2: E2
select and apply protective actions to systems in response to identified risks and system information	Unit 2: D7
communicate potential security concerns clearly to others	Unit 2: E3
handle security-related information in line with policies and procedures for privacy and confidentiality	Unit 2: E4

Pre-Accreditation Draft

DfE WRP3 Prepare, configure and assure readiness of digital systems to meet user needs	
DfE Digital Systems and Data V Level subject content statement	**Unit in Pearson qualification**
the purpose of testing digital systems and the role of quality assurance in maintaining system performance, security and service reliability	Unit 3: A1; Unit 5: A7
categories of testing used in workplace contexts that address system functionality, performance, usability, accessibility and security-related behaviours	Unit 3: C1
methods used to assess system behaviour through comparison of observed outputs with expected outcomes, interpretation of system logs, alerts and performance indicators, and identification of patterns and recurring issues	Unit 3: D1
the impact of system performance, reliability and security issues on user experience, productivity and service continuity	Unit 3: D2; Unit 5: A5.4-A5.6
principles of usability and accessibility and their relevance to system performance, reliability and security for diverse users, including the relationship between interface design, interaction patterns and user effectiveness	Unit 3: C2; Unit 4: D1
the contribution of inclusive and accessible testing practices to reliable digital systems for diverse users	Unit 3: C3
the role of contemporary digital tools in supporting test planning, identification of patterns in system behaviour and summarisation of findings	Unit 3: C4
the role of digital tools and automated and AI-enabled systems in supporting system configuration, testing and identification of patterns in system behaviour, and the need to review outputs to ensure accuracy and suitability	Unit 3: C5
policies relating to data protection, privacy and acceptable system use, and their role in guiding configuration practice: access permissions and user account management, secure configuration and update practices, protection of personal and sensitive information, acceptable use of systems, devices and services	Unit 3: A2
the role of workplace policies, standards and compliance requirements in defining testing scope and quality assurance expectations	Unit 3: A3
the role of system dependencies and component compatibility in ensuring reliable system operation	Unit 3: B1; Unit 5: A4
the impact of system configuration on performance efficiency and resource utilisation	Unit 3: B2; Unit 5: A5.4
the role of controlled, non-live, simulated and training environments in supporting safe and effective configuration practice	Unit 3: A4
the role of recording and documenting test findings accurately and consistently to support review, accountability and improvement decisions	Unit 3: E1
the role of digital tools in supporting system preparation, configuration and checking activities	Unit 3: B3

Pre-Accreditation Draft

the role of clear documentation and communication in supporting accurate, consistent and effective system preparation	Unit 3: E2
the impact of responsible, inclusive and secure configuration practices, and how accessible configuration supports diverse users and reduces barriers to digital participation	Unit 3: B4
environmental and sustainability considerations associated with system performance and efficient use of digital resources	Unit 3: B5
the importance of maintaining system integrity through responsible updates, permissions and security settings	Unit 3: B6
interpret user and system requirements to determine configuration needs and the scope and focus of testing	Unit 3: A5
prepare and configure digital systems to meet defined needs	Unit 3: B7
adjust configuration settings relating to user access, connectivity, storage and security to support system functionality and accessibility	Unit 3: B8
carry out structured tests to confirm system functionality, performance, stability and security-related behaviours	Unit 3: C6
assess system usability and accessibility against stated user needs	Unit 3: C7
review system behaviour and outputs to identify deviations from expected outcomes and apply structured fault-finding approaches where required	Unit 3: D3
record and compare test outcomes against requirements using accurate terminology and structured formats	Unit 3: E3
evaluate test outcomes in relation to defined requirements to determine whether systems are ready for use or require further adjustment	Unit 3: E4
identify and correct configuration settings related to user access, connectivity, storage and security that do not meet defined user requirements	Unit 3: D4
apply routine checks to confirm systems are ready for use: user access and authentication, connectivity and network access, storage availability, software updates and security settings, expected system functionality and performance	Unit 3: C8
apply policies relating to configuration and data protection requirements: secure configuration, access permissions, protection of personal information and software updates	Unit 3: A6
document configuration decisions clearly	Unit 3: E5
communicate configuration outcomes clearly and respond to queries in line with workplace procedures	Unit 3: E6
maintain system integrity through responsible configuration practices, updates, permissions and security settings	Unit 3: B9

Pre-Accreditation Draft

DfE WRP4 Design and create a digital solution to meet defined user needs	
DfE Digital Systems and Data V Level subject content statement	**Unit in Pearson qualification**
the purpose of analysing user needs and requirements when designing digital solutions	Unit 4: A1; Unit 5: C3
approaches used to define problems, determine solution scope and identify constraints, including identifying user needs and requirements, distinguishing between essential and desirable features, identifying assumptions and dependencies, recognising technical, organisational and resource constraints, distinguishing between stated requirements and underlying user needs	Unit 4: A2
how digital systems, components and processes influence the feasibility and structure of proposed solutions, including trade-offs between functionality, complexity and maintainability	Unit 4: B1
the role of automated and AI-enabled systems in supporting solution design, including generating, refining and evaluating solution approaches, and the need to assess the suitability and limitations of outputs	Unit 4: E1
the role of structured logic and step-by-step processes in designing digital solutions to define how inputs, processes and outputs are organised, including the relationship between logic structure and predictability of outcomes	Unit 4: C1
principles of algorithms, and structured coding approaches used to represent, sequence and control solution logic within digital designs	Unit 4: C2
the purpose and characteristics of low-code and block-based development approaches, including how they support rapid prototyping, iterative design and early-stage exploration of digital solution ideas	Unit 4: C3
principles, concepts and approaches underpinning digital design and structured logic in low-code and block-based environments, including abstraction, decomposition, sequencing, selection and iteration, and how these support the development of reliable and maintainable digital solutions	Unit 4: C4
principles of user experience and user interface design that support usability and accessibility, including the relationship between interface design and user behaviour	Unit 4: D1
the role of requirements, assumptions and success criteria in shaping solution proposals, including validation of assumptions and their impact on solution effectiveness	Unit 4: A3
the purpose of low-fidelity representations in communicating solution ideas during early stages of design	Unit 4: D2
policies and procedures relating to accessibility, data protection, security and responsible design and their influence on solution proposals: designing for accessibility and diverse user needs, protection and appropriate use of	Unit 4: E2

Pre-Accreditation Draft

personal and sensitive information, secure authentication and access control, responsible and ethical use of automated and AI-enabled systems	
governance requirements relevant to digital solutions that use automated and AI-enabled systems	Unit 4: E3
potential risks associated with automated decision-making in digital systems and their implications for users and organisations, including limitations of automated decision-making and the need for human oversight	Unit 4: E4
the relationship between user needs, workplace context and effective digital solution design	Unit 4: A4
the contribution of structured problem-solving and logical thinking to robust solution proposals	Unit 4: B2; Unit 5: C1
how design decisions influence usability, accessibility and system behaviour in digital solutions	Unit 4: D3
the role of analysis and planning in reducing risk during later stages of development	Unit 4: B3
the importance of aligning proposed solutions with workplace policies and operational constraints relating to data protection, security, accessibility and acceptable system use: protection and appropriate use of personal and sensitive information, secure authentication and access control, accessibility and the needs of diverse users, acceptable use of systems, devices and services, technical, organisational and resource constraints that affect solution feasibility and implementation	Unit 4: E5
the implications of incorporating automated and AI-enabled processes into digital solutions	Unit 4: E6
the importance of oversight, accountability and transparency in digital solution design	Unit 4: E7
the role of documentation and shared understanding in enabling development decisions	Unit 4: B4; Unit 5: C2.4; Unit 5: C3.4
sustainability considerations in digital solution design: efficient use of resources, energy consumption and device lifecycle	Unit 4: F1
interpret defined user needs and requirements to inform solution design	Unit 4: A5
analyse a problem to identify inputs, outputs, constraints and success criteria	Unit 4: A6
structure a proposed digital solution using logical steps and processes	Unit 4: C5
design solution concepts that consider system behaviour, user interaction and accessibility	Unit 4: D4
produce a clear and structured solution proposal suitable for development	Unit 4: B5
use appropriate development tools, environments and structured inputs, e.g. prompts for automated and AI-enabled systems, to create, refine or represent a digital solution in line with defined requirements	Unit 4: C6
represent solution ideas using specified technical formats (e.g. documents, presentations, spreadsheets, databases)	Unit 4: D5

Pre-Accreditation Draft

justify design decisions in relation to user needs and requirements and governance considerations	Unit 4: E8
document assumptions, decisions and constraints clearly and accurately	Unit 4: F2
communicate proposed solutions clearly to technical and non-technical audiences	Unit 4: F3

Core knowledge and understanding

DfE Digital Systems and Data V Level subject content statement	Unit in Pearson qualification
the main components of digital systems; hardware, software, network infrastructure, data storage and user interfaces, and their roles within system structure	Unit 5: A1
the role of operating systems, user accounts and access controls in enabling secure and effective system use	Unit 5: A2
configuration requirements relating to user accounts, access permissions, connectivity, storage and security settings, including dependency relationships between configuration settings and system behaviour, and the importance of consistency in configuration practices	Unit 3: B8; Unit 3: D4; Unit 3: B9; Unit 5: A4
the relationship between workplace requirements, user needs, configuration decisions, and system performance, usability and security	Unit 5: A5
configuration-related risks arising from misconfigured access permissions, weak authentication settings, unpatched software, exposed network services and insecure default configurations, and their potential impact on systems and users	Unit 5: A5.7
the relationship between defined requirements, test outcomes and decisions about system readiness for deployment and continued use, including defined performance thresholds and trade-offs between performance, usability and security	Unit 5: A7
the nature and causes of technical faults in digital systems, including how faults arise from hardware, software, network and user-related factors, and how system behaviour can be interpreted in relation to expected outcomes to support fault identification and resolution	Unit 5: A6.1-A6.2
structured approaches to diagnosing and resolving faults, including the role of diagnostic tools, system information and logical processes in supporting accurate identification, decision making, escalation and restoration of system functionality, and the consequences of inaccurate diagnosis or delayed action	Unit 5: A6.3
principles of safe, secure and responsible practice when diagnosing and resolving faults: protection of personal and sensitive information, confidentiality and privacy, system integrity and availability, legal and ethical responsibilities, and consideration of the impact of actions on users, services and organisations	Unit 5: B1

Pre-Accreditation Draft

the implications of using automated and AI-enabled systems in decision-making, including limitations, bias and the need for human oversight	Unit 4: E4; Unit 5: B2
the role of communication in technical support, including how information is gathered, interpreted and conveyed to support accurate identification and resolution of issues and effective service delivery	Unit 5: B4
how communication approaches influence clarity, efficiency and user experience, including the need to adapt communication to meet diverse user needs and to distinguish between communication-based support and technical troubleshooting activities	Unit 5: B4; Unit 5: B4.3-B4.4; Unit 5: B4.9
principles of professional, ethical, clear and responsible communication when handling technical information: accuracy and consistency of information, use of appropriate technical and non-technical language, maintaining confidentiality and respecting privacy, adapting communication to audience needs, responding appropriately to user queries and expectations	Unit 4: F3; Unit 5: B4.2, B4.4-B4.7
the role of collaboration in developing digital solutions, including how different roles, perspectives and forms of expertise contribute to decision making and the quality of proposed solutions, and how structured approaches to collaborative working support effective and consistent outcomes	Unit 5: C2
how user needs are identified, interpreted and translated into digital solution designs, including the role of feedback, iteration and shared understanding in refining solutions	Unit 5: C3
principles of problem solving, programming logic and digital solution design, including abstraction, decomposition, sequencing, selection and iteration, and structured approaches used to develop, test and refine digital solutions	Unit 4: C4; Unit 5: C1; Unit 5: C4
the role of prompts and structured inputs in generating outputs from automated and AI-enabled systems, including how prompt design influences the relevance, accuracy and limitations of generated outputs and the broader social and ethical implications of automated and AI-enabled systems and their outputs	Unit 4: E1; Unit 4: C6; Unit 3: C5; Unit 5: B3
ethical, legal and sustainability considerations relevant to digital practice, including intellectual property rights, ownership, attribution and the responsible use of automated and AI-enabled systems and their outputs	Unit 4: E3; Unit 5: C5
the influence of constraints, including technical, organisational and resource factors, on collaborative decision making and digital solution design, and the importance of inclusive and responsible collaboration in achieving effective outcomes	Unit 5: C2.3-C2.6

Pre-Accreditation Draft

Mapping between work-related purposes and Pearson assessments	
DfE Digital Systems and DataV Level subject work-related purpose (WRP)	**Unit in which WRP is assessed**
WRP1: Prepare, analyse, interpret and present data from different sources to support conclusions and decision making	Unit 1
WRP 2: Apply security protocols and interpret system information to detect and escalate cyber security concerns	Unit 2
WRP 3: Prepare, configure and assure readiness of digital systems to meet user needs (optional)	Unit 3
WRP 4: Design and create a digital solution to meet defined user needs (optional)	Unit 4

Pre-Accreditation Draft

Pre-Accreditation Draft

November 2026

For information about Pearson Qualifications, including Pearson Vocational qualifications visit qualifications.pearson.com

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

VAT Reg No GB 278 537121