T-LEVELS | IfATE Institute for Apprenticeships and Technical Education

T LEVEL

Technical Qualification in Digital Support and Security

Specification

First teaching from September2025

Version 1.0 – May 2025

Pearson

T-LEVELS | IfATE Institute for Apprenticeships and Technical Education

T Level Technical Qualification in Digital Support and Security (Level 3)

Specification

First teaching September 2025

Version 1.0 May 2025

Pearson

About Pearson

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

This specification is Version 1.0

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

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

Publication code VQ000477

Contents

1 Introducing the qualification

T Level programme

T Levels are two-year, Level 3 study programmes that follow the study of GCSEs and Technical Awards and offer an alternative to A Levels and Apprenticeships.

T Levels combine classroom theory, practical learning and a minimum 315 hours of industry placement with an employer. The work placement ensures students have real experience of the workplace.

T Level programmes are developed in collaboration with employers so that the content meets the needs of industry and prepares students for work. T Levels provide the knowledge and experience needed to progress to highly skilled employment, an Apprenticeship or higher-level study, including university.

Understanding the Specification and Administrative Guide

This specification should be read in conjunction with the Administrative Guide for Delivery and Assessment. The specification contains all the information you need to teach the Technical Qualification, including content and assessment details. The Admin Guide contains the information and references you need to register as a provider, register students and administer their results. It also contains grading information and information on resources.

What is the Technical Qualification (TQ)?

The *T Level Technical Qualification in Digital Support and Security* is the main classroom-based element of the T Level. Students will learn using a curriculum that has been shaped by industry experts.

During the two-year programme, students will acquire the core knowledge that underpins each industry. They will develop occupationally specific skills that will allow them to enter skilled employment within a specific occupation.

Technical Qualification and Outline Content

The Outline Content for the *T Level Technical Qualification in Digital Support and Security* has been produced by T Level panels of employers, professional bodies and Providers. It is based on the Apprenticeship Standards.

Pearson has used the Outline Content to form the basis of the Technical Qualification specification. This includes:

- elaboration of the Outline Content to produce a specification that gives Providers an accurate interpretation of what needs to be taught and assessed
- enabling students to achieve threshold competence in relation to the Occupational Specialism components
- the integration of English, maths and digital competencies.

English, Maths and Digital competencies

English, Maths and Digital competencies are signposted against Occupational Specialism content. This is because these competencies are best enhanced when students are developing the knowledge and skills they need for threshold competence. The signposting suggests the content areas where the competencies can best be developed by students in the course of their learning. The competencies are indicated by abbreviations (e.g. E1) – and the explanation of the abbreviations is contained in Appendix 1.

Employer and Provider panels

Pearson engaged with employer and Provider panels throughout the development of the Technical Qualification. This ensured:

- the content gives students quality preparation to help them progress
- assessments are realistic and assess the knowledge and skills that are important to employers
- the Technical Qualification meets the needs of Providers.

Pearson is grateful to all university and further education lecturers, teachers, employers, professional body representatives and other individuals who have generously shared their time and expertise to help us develop these new qualifications.

Qualification purpose

This Technical Qualification is for T Level students who are undertaking the *T Level in Digital Support and Security*. It is intended for students who want to progress to a career in the *digital* sector.

The purpose of the *T Level Technical Qualification in Digital Support and Security* (Level 3) is to ensure students have the knowledge and skills needed to progress into highly skilled employment, an Apprenticeship or higher-level study, including university, within the specialist area of Digital Support and Security.

At the end of the Technical Qualification, students are expected to demonstrate threshold competence, meaning that they have gained the core knowledge and skills related to Digital Support and Security and are well placed to develop full occupational competence, with additional development and support once in employment in the digital sector.

Student profile and progression

Students undertaking this Technical Qualification will be 16–19 years old and in full-time education.

The typical student has:

- a clear idea about the industry sector in which they wish to pursue a career
- an idea of the type of job role they would like to explore as a career.

This Technical Qualification aligns to Level 3 Apprenticeships in Digital Infrastructure Engineering (infrastructure technician) Network Cabling (network cable installer), Digital Support (digital support technician) and Cyber Security (cyber security technician). The qualification therefore supports progression to entry-level job opportunities in Digital Support and Security.

Job roles could include:

- digital support technician
  - digital applications technician
  - digital service technician
- infrastructure technician
- IT solutions technician
  - hardware solutions
  - software solutions
- network cable installer
- cyber security technician.

Alternatively, students could progress to Level 3 Apprenticeships such as those mentioned above to develop and gain certification of full occupational competence, or they could progress to higher-level Apprenticeships such as the Level 4 Digital Infrastructure Engineer, Network Engineer, Applications Support Lead, Cyber Security Technologist, depending on their skills or experience.

Where students may not have access to an Apprenticeship or would prefer a more academic route, they could progress to relevant Higher National Certificate (HNC) or Higher National Diploma (HND) programmes or degree programmes.

Students must check the entry requirements for each degree programme with the relevant higher education provider.

2 Qualification summary and structure

Summary

Qualification title	T Level Technical Qualification in Digital Support and Security (Level 3)
Qualification number (QN)	610/5799/X
First teaching	September 2025
This qualification replaces	603/6901/2 T Level Technical Qualification in Digital Support Services
Total Guided Learning Hours (GLH)	1200 hours (600 hours core)
Total Qualification Time (TQT)	1320 hours (660 hours core)
Occupational Specialism(s)	• Digital Infrastructure (600 GLH, 660 TQT) • Network Cabling (600 GLH, 660 TQT) • Digital Support (600 GLH, 660 TQT) • Cyber Security (600 GLH, 660 TQT)
Components and weighting	Core Paper 1 = 30% of core (15 % of total) Core Paper 2 = 30% of core (15 % of total) Core ESP = 40% of core (20 % of total) Core Component = 50% of total Occupational specialism = 50% of total
Recommended age range	16–19
Grading information	Core and Employer Set Project (ESP) components are graded A*–E or Unclassified. The Occupational Specialism (OS) components are graded Pass, Merit, Distinction or Unclassified. The overall grading is on a scale of Pass, Merit, Distinction, Distinction* or Unclassified. The overall grade is awarded by the Institute for Apprenticeships and Technical Education (IfATE).

Qualification title	T Level Technical Qualification in Digital Support and Security (Level 3)
Entry requirements	There are no formal prior learning requirements. It is the Provider's responsibility to ensure students recruited have a reasonable expectation of success. Students are most likely to succeed if they have qualifications at Level 2 (for example, 5 GCSEs at grade 4 and above including English and maths or a vocational Tech Award pass at Level 2). Students may demonstrate the ability to succeed in various ways. For example, they may have relevant work experience or may have shown specific aptitude through diagnostic tests or other non-educational experience.
Assessment	• The core and ESP components are externally set and marked by Pearson. • The OS components are set by Pearson. These are externally marked by Pearson.

Assessment Structure

The *T Level Technical Qualification in Digital Support and Security* has two mandatory components.

1. Core component

This component covers the underpinning knowledge, concepts and skills that support threshold competence in the digital industry.

The content for the Core component is provided in *Section 3*.

Assessment component	Assessment method	Duration	Marks	Weighting	Timetable	Availability
Core Paper 1	Written examination	2 hours 15 minutes	90	30%	Set date/time	June/ November
Core Paper 2	Written examination	2 hours 15 minutes	90	30%	Set date/time	June/ November
Employer Set Project	Externally set project	14 hours 30 minutes	89-100	40%	Set date/time	May/ November

2. Occupational Specialism component

There are four Occupational Specialism components in this Technical Qualification.

These components cover the Occupational Specialism knowledge and skills required to demonstrate threshold competence for the specialism. The Occupational Specialism is assessed by a skills-related project that synoptically assesses the Performance Outcome skills and associated underpinning knowledge.

The content for the Occupational Specialism component is provided in *Section 4*.

Assessment component	Assessment method	Duration	Marks	Weighting	Timetable	Availability
Digital Infrastructure	Externally set project	37 hours 30 minutes	99	100%	Windowed	March to May
Network Cabling	Externally set project	37 hours 30 minutes	111	100%	Windowed	March to May
Digital Support	Externally set project	37 hours 30 minutes	99	100%	Windowed	March to May
Cyber Security	Externally set project	37 hours 30 minutes	99	100%	Windowed	March to May

What does the qualification cover?

The Technical Qualification content has been designed from the Outline Content created by the Institute for Apprenticeships and Technical Education and the Digital T Level panel.

We have used the Outline Content to create the Technical Qualification specification and assessment, which have been validated by our own panel of employers and Providers to ensure they are appropriate for the progression routes identified.

Students learn about the following topics:

- Problem solving
- Introduction to digital support
- Data
- Legislation and regulatory requirements
- Business context
- Emerging issues
- Digital environments
- Security.

3 Core Component

The content of the Core component has the core skills mapped to where there are opportunities to develop them. The competencies and skills are not expected to be developed at every point where they are mapped, but using this guidance teachers will embed them into teaching to prepare students for the assessments in the Core component.

The core skills are assessed through the Employer Set Project. The core skills for this Core component are as follows.

1. Be able to reflectively evaluate
2. Communicate information clearly to a technical and non-technical audience
3. Work with stakeholders to consider options to meet requirements
4. Develop software/Create an artefact
5. Apply a logical approach to solving problems:
    - identify and resolve faults
    - propose a solution to a digital support problem
6. Ensure activity mitigates risks to security.

Content

Core paper 1

Content area 1: Problem solving	
Students will solve digital support and security problems that form a complete solution or a sub-part of a solution. Students will use problem-solving skills to analyse problems and to identify solutions that can be represented as systems, processes, relationships or organisations of data.	
1.1 Computational thinking	
1.1.1	Know the definition and understand the purpose of computational thinking.
1.1.2	Know when to use computational thinking.
1.1.3	Know and understand the benefits and drawbacks of using computational thinking.
1.1.4	Know the components of computational thinking: • decomposition • pattern recognition • abstraction • algorithmic design.
1.1.5	Know and understand the benefits and drawbacks of using the components of computational thinking.
1.1.6	Know and understand the purpose of decomposition.
1.1.7	Know the tasks of decomposition: • identify the main features of a problem • characterise each identified feature • break problems down into smaller, more manageable parts • break solutions down into smaller, more manageable parts.
1.1.8	Be able to use decomposition for problem solving.
1.1.9	Know and understand methods to represent decomposition: • block diagrams • information flow diagrams • flowcharts • written descriptions.
1.1.10	Be able to use methods to represent decomposition.
1.1.11	Know and understand the purpose of pattern recognition.

1.1.12	Be able to use pattern recognition for problem solving: • find and interpret trends and similarities within and between problems and processes • find and interpret common features between a given problem and existing solutions • make predictions and assumptions based on identified patterns.
1.1.13	Know and understand the purpose of abstraction.
1.1.14	Know and understand the tasks of abstraction: • identify information that is needed • filter out unnecessary details • hide details of internal workings.
1.1.15	Be able to use abstraction: • what inputs are needed • what the expected outputs and outcomes are • things that will vary • things that will remain constant • key actions the solution must perform • repeated processes the solution will perform.
1.1.16	Be able to use abstraction in problem solving.
1.1.17	Understand the interrelationships between components of computational thinking and make judgements about the suitability of using the components in digital support and security.
1.2 Algorithmic design	
1.2.1	Know the definition and understand the characteristics and purpose of algorithms

1.2.2	Know and understand methods to express algorithms:
	• flowcharts:
	  ○ terminators
	  ○ processes
	  ○ sub-processes
	  ○ decisions
	  ○ inputs/outputs
	  ○ arrows
	  ○ labels
	• written descriptions using hierarchical markers to indicate sequence.

1.2.3	Know and understand the benefits and drawbacks of expressing algorithms in flowcharts.
1.2.4	Know and understand the benefits and drawbacks of expressing algorithms in written descriptions.

1.2.5	Know and understand actions to control ordering of steps in algorithms: • sequence • selection • iteration.
1.2.6	Be able to determine the purpose of an algorithm and how it works.
1.2.7	Be able to determine the output of an algorithm given an input.
1.2.8	Be able to identify errors in an algorithm.
1.2.9	Be able to correct errors in an algorithm.
1.2.10	Be able to design algorithms and solutions that use actions.
1.3 Strategies	
1.3.1	Know the different approaches to solving problems and understand their purpose and when they are used: • top-down • bottom-up • modularisation.
1.3.2	Know the benefits and drawbacks of using the different approaches to solving problems.
1.3.3	Understand the purpose of root cause analysis and when it is used.

1.3.4	Know and understand approaches to root cause analysis:
	• five whys
	• failure mode and effects analysis (FMEA)
	• event tree analysis (ETA)
	• actions to take after using root cause analysis:
	  ○ log
	  ○ close
	  ○ escalate to an appropriate manager, specialist or external third party.

1.3.5	Know and understand the process of the high-level problem-solving strategy: • define the problem • gather information • analyse the information • make a plan of action • implement a solution • review the solution.
1.3.6	Know the definition of a digital incident, in incident management: • a single unplanned event • that disrupts service operations • that negatively impacts service quality.

1.3.7	Know the definition of a digital problem, in incident management, as the cause of the incident.
1.3.8	Know and understand the process of incident management: • detection: report, record, prioritise • response: identify owner, resolve and restore, record resolution • intelligence: record lessons, identify cause, share lessons.
1.3.9	Understand the interrelationships between problems and problem-solving strategies and make judgements about the suitability of strategies for solving the problems in digital support and security.

Content area 2: Introduction to digital support	
Students will analyse digital support and security problems that may involve hardware, software, people, processes and data. Students will use a variety of tools and techniques when developing a complete solution or a sub-part of a solution.	
2.1 Infrastructure	
2.1.1	Know and understand the purpose of data held in routing tables: • static addresses • dynamic addresses • network ID • subnet mask • next hop • interface (device) designation.
2.1.2	Be able to interpret data from routing tables.
2.1.3	Know and understand the purpose of console applications that display TCP/IP network configurations: • ipconfig/ifconfig.
2.1.4	Be able to interpret data from console applications.
2.1.5	Know and understand the purpose of a firewall and the role it has in securing networks.
2.1.6	Know and understand the purpose of: • securing a firewall's administrator access • setting precedence rules for ALLOW and BLOCK.
2.2 Cabling	
2.2.1	Know and understand the characteristics of cable types and where they are used: • unshielded twisted pair (UTP) • shielded twisted pair (STP) • coaxial • fibre-optic.

2.2.2	Know a definition for Ethernet, understand its purpose, and where it is used.
2.2.3	Know and understand characteristics of cable standards in the context of ethernet: • CAT 5e • CAT 6 • CAT 7.
2.2.4	Know and understand metrics to compare cable standards in the context of ethernet: • bandwidth • maximum length.
2.2.5	Know and understand the benefits and drawbacks of cable standards.
2.3 Unified communications	
2.3.1	Understand communication types, their purposes and functions: • VoIP (Voice over Internet Protocol) • SIP (Session Initiation Protocol).
2.3.2	Understand the relationship between VOIP and SIP.
2.3.3	Know definitions of each network metric: • speed • bandwidth • latency • jitter • packet loss.
2.3.4	Know and understand the relationships between the network metrics and their impact on user experience when communicating on a network.
2.3.5	Know and understand the purpose of codecs: • compressing data • uncompressing data.
2.3.6	Know the different types of codecs, their purpose and the types of algorithm they use: • MPEG-4 (video, lossy/lossless) • MP3 (audio, lossy) • FLAC (audio, lossless).
2.4 Support	
2.4.1	Understand the needs of users when selecting, configuring and testing digital system components: • hardware: cores, memory, secondary storage, clock speed, connectivity • operating systems: graphical, text-based, multi-tasking, single user, multi-user, virtual machine

	• software: database, spreadsheet, word processor, presentation, communication, browser.
2.4.2	Be able to select, configure and test digital system components.
2.4.3	Understand the interrelationships between the components and make judgements about the suitability of components in the context of meeting user's needs.
2.4.4	Know fault indicators and understand their purpose and when they are used to identify hardware and software faults: • error numbers • error messages • beep codes • blink codes.
2.4.5	Be able to interpret fault indicators to diagnose problems in hardware and software.
2.4.6	Be able to interpret technical documentation to diagnose problems in hardware and software.
2.5 Testing	
2.5.1	Understand the reasons for testing individual components before putting them together into a solution: • software • hardware • data • interfaces • resulting service (final product).
2.5.2	Know a definition of testing methods and understand their purpose, benefits and drawbacks, and when they are used: • concept • unit • boundary • integration • performance • system • acceptance • usability • regression • load/stress • closed box • open box.
2.5.3	Be able to use testing methods.

2.5.4	Know and understand the purpose of automation methods and when they are used: • macros • scripts.
2.5.5	Know a definition for types of test data and understand the purpose of test data and when it is used: • valid • invalid • boundary • erroneous.
2.5.6	Be able to create test data.
2.5.7	Know and understand the steps and structure of a test plan and when it is used: • identifying tests to be carried out • describing the purpose of the identified test • identifying test data to be used • describing the expected results • recording actual results.

2.5.8	Know and understand methods to check the believability and accuracy of results:
	• logical reasoning:
	  ○ all relevant and appropriate inputs are included, without bias in selection
	  ○ results make sense in relationship to the inputs
	• verification by subject matter expert
	• use of test plans.

2.6 Using data in digital support	
2.6.1	Understand how tabular data is organised: • worksheet • row • column.
2.6.2	Know the definition of validation checks and understand their purpose and when each is used: • presence • length • range • type • format.

2.6.3	Know techniques to interrogate data and understand their purpose and when they are used: • order by key field • sort on a field(s) • filter on field(s) • arithmetic functions • SUM, MIN, MAX, AVERAGE • IF, COUNTIF
2.6.4	Be able to use techniques to interrogate data in spreadsheets.
2.6.5	Understand the purpose of saving data to and importing data from text-based files.
2.7 Using diagrams in digital support	
2.7.1	Understand data flow diagrams (DFD), their purpose, and when they are used.
2.7.2	Know and understand how data flow is expressed in DFDs: • data sources • data destinations • processes • data stores • arrows • labels. See symbols in *Appendix 2*.
2.7.3	Be able to interpret DFDs that represent systems.
2.7.4	Be able to create and complete DFDs that represent systems.
2.7.5	Understand information flow diagrams and their purpose and when they are used.
2.7.6	Know and understand how information flow is expressed in information flow diagrams: • boxes • arrows • labels. See symbols in *Appendix 2*.
2.7.7	Be able to create and complete information flow diagrams to represent systems.
2.7.8	Be able to interpret information flow diagrams that represent systems.

2.8 Risk and risk assessment	

2.8.1	Know and understand that risk is assessed in terms of likelihood and severity at different levels in a five-by-five matrix:
	• Likelihood:
	  ○ improbable
	  ○ remote
	  ○ occasional
	  ○ probable
	  ○ frequent.
	• Severity:
	  ○ negligible
	  ○ marginal
	  ○ moderate
	  ○ critical
	  ○ catastrophic.

2.8.2	Be able to interpret and create a risk assessment matrix.
2.8.3	Know and understand the purpose of risk assessment documentation: • ensure continuity of service • ensure health and safety of people • ensure regulatory compliance.
2.8.4	Know and understand risk assessment documentation: • a description of the risk • who/what might be harmed/damaged • a description of how the harm/damage might occur • the mitigation already in place • details of additional required mitigation • who is responsible for carrying out the mitigation? • the due date for completion.
2.8.5	Be able to interpret and create risk assessment documentation.
2.9 Project management methodologies and tools for digital support logistics	
2.9.1	Know and understand the components, benefits and drawbacks of methodologies for managing digital projects: • Waterfall • Agile.
2.9.2	Know and understand benefits and drawbacks of diagrammatic techniques for project management: • Program Evaluation Review Technique (PERT) • Precedence tables • Gantt • Kanban • Critical Path Analysis (CPA).

2.9.3	Be able to interpret and draw diagrams for project management.
2.9.4	Understand the interrelationships between projects, management methodologies and diagrammatic techniques, and make judgements about their suitability.
2.10 Strategies for responding to support issues	
2.10.1	Know and understand the application, benefits and drawbacks of the four stages of Kolb's Experiential Learning Cycle: • concrete experience • reflective observation • abstract conceptualisation • active experimentation.
2.10.2	Know and understand the application, benefits and drawbacks of the six stages of Gibbs' Reflective Cycle: • description • feelings • evaluation • analysis • conclusion • action plan.
2.10.3	Know and understand the process, benefits and drawbacks of concept mapping: • main idea and central point of focus • individual concepts: hardware, software, people, information, processes • relationships (verbs).
2.10.4	Be able to interpret and create concept maps for digital support situations.
2.10.5	Know and understand the use of, and the benefits and drawbacks of, the design thinking process: • empathise • define • ideate • prototype • user feedback • repeat prototype/user feedback.
2.11 Sources of knowledge	
2.11.1	Know and understand sources of knowledge: • literature: textbooks, manuals, supplier literature • professionals: conferences, managers, colleagues • websites: wikis, blogs, forums • media: social media, podcast, video • observation: dashboards, inspection.

2.11.2	Reliability and validity of sources:
	• factors:
	  ○ bias/subjectivity
	  ○ evidence/expertise
	  ○ publication date
	• corroboration from other sources.

2.11.3	Make judgements about the relationships between the sources of knowledge and the factors that impact reliability and validity.

Content area 3: Data	
Students will develop fundamental knowledge and understanding of data relevant to digital support and security, in order to communicate with other professionals. Students will understand how to store, access, quality assure, manipulate, analyse and process data.	
3.1 Data, information and knowledge	
3.1.1	Know and understand the differences and relationships between: • data • information • knowledge.
3.1.2	Know and understand sources for generating data: • human: surveys, forms • Artificial Intelligence (AI)/machine learning: dangers of feedback loop • sensors: temperature, accelerometer, vibration, sound, light, pressure • Internet of Things (IoT): smart objects (thermostats, lights, security camera, trackers) • transactions: customer data, membership, timing, basket
3.1.3	Know and understand ethical data practices and the metrics to determine the value of data: • quantity • timeframe • source • veracity.
3.1.4	Understand how organisations use data and information: • analysis to identify patterns • system performance analysis: load, outage, throughput, status • user monitoring: login/logout, resources accessed • targeted marketing: discounts, upselling • threat/opportunity assessment: competitors, security, compliance.
3.1.5	Understand the interrelationships between data, information and the way it is generated and make judgements about the suitability of data, information and the way it is generated in digital support and security.

3.2 Methods of transforming data	
3.2.1	Know and understand methods of transforming data: • manipulating • analysing • processing.
3.3 Data taxonomy	
3.3.1	Know the definition of each category, understand its purpose, and understand that data is categorised as: • quantitative • qualitative.
3.3.2	Know the definition for structured data, understand its purpose, and understand that quantitative data is structured.
3.3.3	Know the definition for unstructured data, understand its purpose, and understand that qualitative data is unstructured.
3.3.4	Know the definition for each representation and understand the representations of quantitative data: • discrete values • continuous values • categorical values.
3.3.5	Know and understand the properties of qualitative data: • stored and retrieved only as a single object • codified into structured data.
3.3.6	Understand the interrelationships between data categories data structure and transformation and make judgements about the suitability of data categories, data structure and transformation in digital support and security.
3.4 Data types	
3.4.1	Know the definition of common data types and understand their purpose and when each is used: • integer • real • character • string • Boolean • date • Blob.
3.4.2	Understand the interrelationships between structured data, unstructured data and data type.
3.4.3	Understand the interrelationships between data type and data transformation.

3.4.4	Be able to make judgements about the suitability of using structured data, unstructured data, data types, and data transformations in digital support and security.
3.5 Data formats	
3.5.1	Know the definition of common data formats and understand their purpose and when each is used: • JSON • Text file • CSV • UTF-8 • ASCII • XML.
3.5.2	Understand the interrelationships between data format and data transformation, and make judgements about the suitability of using data formats in digital support and security.
3.6 Structures for storing data	
3.6.1	Understand the role of metadata in providing descriptions and contexts for data.
3.6.2	Know the definition of file-based and directory-based structures and understand their purposes and when they are used.
3.6.3	Know the definition of hierarchy-based structure and understand its purpose and when it is used.
3.6.4	Understand the interrelationships between storage structures and data transformation.
3.7 Data dimensions and maintenance	
3.7.1	Know the definitions of the six Vs (dimensions) and understand the six Vs (dimensions) of Big Data and their impact on gathering, storing, maintaining and processing: • volume • variety • variability • velocity • veracity • value.
3.7.2	Know the definition of Big Data and understand that it has multiple dimensions.
3.7.3	Understand the impact of each dimension on how data is gathered and maintained.

3.7.4	Know the definitions of data quality assurance methods and understand their purpose and when each is used: • validation • verification • reliability • consistency • integrity • redundancy.
3.7.5	Know and understand factors that affect how data is maintained: • time • skills • cost.
3.7.6	Understand the interrelationships between the dimensions of data, quality assurance methods and factors that impact how data is maintained and make judgements about the suitability of maintaining, transforming and quality assuring data in digital support and security.
3.8 Data systems	
3.8.1	Know the definition of data wrangling and understand its purpose and when it is used.
3.8.2	Know and understand the purpose of each step of data wrangling: • structure • clean • validate • enrich • output.
3.8.3	Know and understand the purpose of each core function of a data system: • input • search • save • integrate • organise (index) • output • feedback loop.
3.8.4	Know the types of data entry errors and understand how and why they occur: • transcription errors • transposition errors.

3.8.5	Know and understand methods to reduce data entry errors: • validation of user input • verification of user input by double entry • drop-down menus • pre-filled data entry boxes.
3.8.6	Know and understand the factors that impact implementation of data entry: • time needed to create the screens • expertise needed to create screens • time needed to enter the data.
3.8.7	Understand the relationship between factors that impact data entry and data quality and make judgements about the suitability of methods to reduce data entry errors in digital support and security.
3.8.8	Understand the relationship between factors that impact implementation of data entry and make judgements about the suitability of implementing data entry in digital support and security.
3.9 Data visualisation	
3.9.1	Know and understand data visualisation formats and when they are used: • graphs • charts • tables • reports • dashboards • infographics.
3.9.2	Know and understand the benefits and drawbacks of data visualisation formats based on: • type of data • intended audience • brief.
3.10 Data models	
3.10.1	Know the types of data models and understand how they organise data into structures: • hierarchical • network • relational.
3.10.2	Know and understand the factors that impact the selection of data model for organising data: • efficiency of accessing individual items of data • efficiency of data storage • level of complexity in implementation.

3.10.3	Understand the benefits and drawbacks of different data models and make judgements about the suitability of data models based on efficiency and complexity.
3.10.4	Be able to draw and represent data models: • hierarchical models with blocks, arrows and labels • network models with blocks, arrows and labels • relational models with tables, rows, columns and labels.
3.11 Data access across platforms	

3.11.1	Understand the features, purposes, benefits and drawbacks of accessing data across platforms:
	• permissions
	  ○ authorisation
	  ○ privileges
	  ○ access rights
	  ○ rules
	• access mechanisms:
	  ○ role-based access (RBAC)
	  ○ rule-based access control (RuBAC)
	  ○ Application Programming Interfaces (API).

3.11.2	Know and understand the benefits and drawbacks of methods to access data across platforms.
3.11.3	Understand the interrelationships between data access requirements and data access methods and make judgements about the suitability of accessing data in digital support and security.
3.12 Data analysis tools	

3.12.1	Know data analysis tools and understand their purpose and when they are used:
	• storing Big Data for analysis:
	  ○ data warehouse
	  ○ data lake
	  ○ data mart
	• analysis of data:
	  ○ data mining
	  ○ reporting
	• use of business intelligence gained through analysis:
	  ○ financial planning and analysis
	  ○ customer relationship management (CRM):
	  – customer data analytics
	  – communications.

3.12.2	Understand the interrelationships between data analysis tools and the scale of data.

Core paper 2

Content area 4: Legislation and regulatory requirements	
4.1 Legislation	

4.1.1	Understand the key points and implications to employers of the relevant health and safety legislation:
	• Health and Safety at Work Act:
	  ○ key points:
	  – provide a safe working environment
	  – ensure staff are properly trained
	  – adequate welfare provision
	  – provide relevant information, instruction and supervision
	• manual handling operations:
	  ○ key points:
	  – avoid hazardous manual handling operations as far as possible
	  – assess any hazardous manual handling operations
	  – provide information on load and centre of gravity
	  – reduce the risk of injury so far as is reasonably practicable
	• work at height regulations:
	  ○ key points:
	  – make sure the work is properly planned, supervised and carried out by competent people
	  – do as much work as possible from the ground
	  – ensure workers can get safely to and from where they work at height
	  – ensure equipment is suitable, stable and strong enough for the job
	  – provide protection from falling objects
	  – consider emergency evacuation rescue procedures
	• display screen equipment:
	  ○ implications to employers:
	  – conduct a display screen equipment workstation assessment
	  – reduce risks including making sure workers take breaks from display screen equipment work
	  – provide an eye test if an employee asks for one
	  – provide training and information for employees.

4.1.2	Understand the health and safety risks and preventative measures of working with digital systems:
	• possible risks:
	  ○ using display screen equipment
	  ○ working at heights
	  ○ cable installation (ground level, onto walls)
	  ○ manual handling
	  ○ health and safety requirements

	• methods of mitigating risk:
	  ○ adequate training
	  ○ safe working environment
	  ○ suitable provision of relevant safety equipment
	  ○ safe working practices
	  ○ suitable provision of relevant information, instruction and supervision.

4.1.3	Understand Data Security and Protection legislation, including their effect on organisations and individuals:
	• Data Protection Act/General Data Protection Regulations:
	  ○ purpose of legislation
	  ○ eight principles.

4.1.4	Understand Computer Misuse legislation: • the principles of the Computer Misuse Act (CMA) 1990 • consequences for company and employee • employee awareness • types of crimes covered by legislation.

4.1.5	Understand Equality legislation:
	• the nine protected characteristics
	• types of discrimination:
	  ○ direct
	  ○ indirect
	  ○ harassment
	  ○ victimisation
	• where individuals are protected
	• when to take action against discrimination
	  ○ time limits for claims.

4.1.6	Understand Intellectual Property legislation: • unregistered designs • registered designs • patents.
4.1.7	Understand Electrical Waste legislation: • Waste Electrical and Electronic Equipment Regulations • safe disposal • environmentally responsible disposal.
4.1.8	Understand the interrelationships between digital support and security and digital legislation, and make judgements about the impact on organisations, society and individuals.
4.1.9	Know that international law applies to some offences: • international law in cyberspace • international law and surveillance.

4.2 Guidelines	

4.2.1	Know the sources of codes of conduct:
	• organisations
	• professional:
	  ○ British Computer Society (BCS)
	  ○ The Institution of Analysts and Programmers (IAP)
	  ○ Chartered Institute of Information Security (CIISec)
	• governmental.

4.2.2	Understand how guidelines in codes of conduct influence professional behaviour:
	• ensure individuals follow policies, procedures and legislation
	• ensure quality of work:
	  ○ minimising risk to the public
	  ○ acting with competence and integrity
	• meeting deadlines
	• effective communication
	• maintaining confidentiality and trust.

4.2.3	Know the sources of digital industry standards: • International Organization for Standardization (ISO) • Web Content Accessibility guidelines (WCAG) • World Wide Web Consortium (W3C®) • Internet Engineering Task Force (IETF) • Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA) • British Standard (BS) • Institute of Electrical and Electronics Engineers (IEEE) • Payment Card Industry Security Standards Council (PCI SSC).

4.2.4	Understand the purpose of acceptable use policies (AUP):
	• purpose of AUP
	• typical content:
	  ○ permitted activities
	  ○ prohibited activities
	  ○ working practices including confidentiality
	  ○ communication etiquette including projecting correct organisation image
	  ○ sanctions/penalties.

4.2.5	Understand the importance of whistleblowing procedures.
4.2.6	Understand the interrelationships between digital support and security and guidelines, and make judgements about the impact on organisations, society and individuals.

Content area 5: Business context	
5.1 Business environment	

5.1.1	Know the purpose and sectors of different types of organisations:
	• purpose of the organisation:
	  ○ providing a service
	  ○ providing a product
	• private sector:
	  ○ Small or Medium-sized Enterprise (SME)
	  ○ Large enterprise
	  ○ Non-governmental organisation (NGO)
	• public sector
	• voluntary/charity
	  ○ not for profit.

5.1.2	Know the names and definitions of different business models: • Business to Customer (B2C) • Business to Business (B2B) • Business to Many (B2M).

5.1.3	Know the different types of stakeholders:
	• internal stakeholders:
	  ○ owners
	  ○ directors
	  ○ employees
	• external stakeholders:
	  ○ customers/clients
	  ○ suppliers
	  ○ shareholders
	  ○ outsourced services
	  ○ investors/funders
	  ○ government.

5.2 Digital value to organisations	

5.2.1	Understand how digital systems are used to support key organisation areas:
	• sales and marketing:
	  ○ better market research
	  ○ better brand promotion including social media
	  ○ online selling
	  ○ contextualising customer behaviour to personalise services offered
	  ○ better customer retention
	  ○ brand differentiation and values
	  ○ use of analytical tools including search and social media analytics

	• research, design and development
	  ○ provision of unique products and services
	• Human Resources:
	  ○ staff records
	  ○ performance management
	  ○ training records
	• operations:
	  ○ enhanced internal communication
	  ○ automation of internal processes
	  ○ automated manufacturing
	  ○ remote working
	  ○ intranet/shared workspace
	  ○ document sharing and online shared storage
	• management:
	  ○ real-time monitoring of key performance indicators:
	  – sales
	  – customers served
	  – units measured
	  – real-time location of assets
	• logistics:
	  ○ automated stock control
	• finance:
	  ○ reduced costs
	  ○ increased revenue
	  ○ better financial reporting via up-to-date information.

5.2.2	Understand how digital systems are used to meet user needs and ensure quality of product/service:
	• appropriate and effective functionality:
	  ○ allows users to do all required tasks
	• reduction of pain points:
	  ○ response time (communication of expected response time, notification of change in response time)
	  ○ complexity of task
	• appropriate accessibility provision
	• compatibility:
	  ○ with internal legacy systems
	  ○ with proposed future systems
	  ○ with external services
	• availability of service:
	  ○ minimise downtime
	  ○ future proofing for update
	• effective end user support:
	  ○ provision of digital support

	• ease of installation: ○ provision of installation package.
5.3 Risk to organisations of using digital systems	

5.3.1	Understand the potential risks to organisations when using digital systems:
	• security breaches:
	  ○ compromised confidentiality
	  ○ loss of integrity
	  ○ reduced availability
	• privacy breaches:
	  ○ personal information
	  ○ business information
	• regulatory and legal non-compliance
	• audience exclusion:
	  ○ biases
	  ○ poor user experience
	• emerging rival technologies
	• technical issues:
	  ○ reliance and system failure
	  ○ system not fit for purpose.

5.3.2	Understand the potential impact of risks to organisations when using digital systems: • legal action • fines • reputational damage • withdrawal of licence to practise • loss of business.
5.4 Technical change management	

5.4.1	Understand the internal factors that trigger change in organisations
	• Internal factors:
	  ○ organisational restructuring
	  ○ expansion
	  ○ downsizing
	  ○ new strategic objectives
	  – diversification
	  – rebranding
	  – additional features or services.
	• Unforeseen or previously unpreventable factors:
	  ○ crises (natural disasters, terrorism, cyber-attacks)
	  ○ system failures/data corruption

5.4.2	Understand the external factors that trigger change in organisations:
	• political:
	  ○ change in government
	  ○ conflict
	  ○ shift in government priorities
	• economic:
	  ○ provision of new services
	  ○ recession
	  ○ inflation
	  ○ interest rates
	  ○ consumer trends
	  ○ new competitors
	  ○ entering new markets
	• social:
	  ○ changes in demographics
	  ○ market/social trends
	  ○ adopting remote working
	  ○ cultural expectations
	• technological:
	  ○ emergence of new technologies
	  ○ retirement of obsolete technologies
	  ○ system failure
	  ○ zero-day vulnerabilities
	• legal:
	  ○ new legislation
	  ○ changes to legislation
	• environmental:
	  ○ sustainability issues
	  ○ pandemics
	  ○ natural disasters.

5.4.3	Understand how organisations can respond to change:
	• new or amended policies
	• new or amended business processes:
	  ○ change in staffing number
	  ○ change in delivery schedules
	  ○ change in opening hours
	• new or amended products or services:
	  ○ completely new products or services
	  ○ next generation products or services
	  ○ minor updates to existing products or services

	• new or improved digital systems:
	  ○ back end systems
	  ○ customer facing systems
	• improved training
	• restructuring:
	  ○ change in management structure
	  ○ re drawing of boundaries.

5.4.4	Understand the processes, benefits and drawbacks of the change management process:
	• identifying type of change:
	  ○ new system
	  ○ amendment to existing system
	• role of Change Advisory Board (CAB):
	  ○ prioritise change requests
	  ○ review change requests
	  ○ stages of approval
	  ○ monitor change process:
	  – collate and analyse change data
	  – check change is implemented
	  – take action to accelerate change
	  ○ provide feedback
	• identifying the changes to be made:
	  ○ using SMARTER objectives (specific, measurable, achievable, realistic, time-bound, evaluated, reviewed)
	• identifying impact of change:
	  ○ measure/forecast positive and negative impact
	  ○ analysis of positive and negative impact
	• allocation of resources:
	  ○ budget
	  ○ time
	  ○ staffing
	  ○ hardware and software
	• identify and communicate potential risks and desired impact(s) to stakeholders:
	  ○ gain acceptance
	  ○ ensure compliance
	• configuration of the new system or process:
	  ○ integration with legacy systems
	  ○ maintaining service during change
	• importance of fully testing new systems:
	  ○ reproducibility of results
	  ○ test environment including hardware and software

	• method of implementing change:
	  ○ parallel
	  ○ phased
	  ○ direct
	  ○ pilot
	• documenting the change process:
	  ○ ensuring requirement traceability, including responsibility and accountability
	  ○ maintaining up-to-date information
	  ○ recording of all decisions
	  ○ retaining change documentation
	  ○ user training manuals
	• importance of rollback planning:
	  ○ back-up methodology
	  ○ back-up location
	  ○ recovery plan
	• identify training needs:
	  ○ new training requirements
	  ○ refresher course
	• identify methods of monitoring progress:
	  ○ post progress review
	• version control.

5.4.5	Understand the factors that determine the feasibility of a digital project:
	• benefits and drawbacks:
	  ○ financial savings
	  ○ cost of implementing change
	  ○ impact on processes, including productivity gains, improved communication and security
	  ○ provision of new products
	  ○ impact on company reputation
	• risks:
	  ○ resistance to change from workforce
	  ○ misuse of new systems
	  ○ inadequate support for new system
	  ○ inadequate knowledge of new system
	  ○ disruption caused by implementation of new systems
	• constraints:
	  ○ budget
	  ○ time
	  ○ human resources and technological resources.

5.5 How digital support roles enable business operations	
5.5.1	Understand roles, responsibilities and required skills when supporting digital infrastructure: • responsibilities: o install, test and maintain components o schedule system updates and communicate changes to end users o maintain optimum system availability o perform recovery and restoration o optimise hardware, software and network performance o apply security measures o troubleshoot problems o escalate issues o work to relevant legislation o design and document system changes • roles: o technician/service desk roles o line support (first to fourth level) o network installation o server support • skills: o problem solving o analytical thinking o use digital tools o communicate effectively o prioritise tasks o teamwork o importance of upskilling.
5.5.2	Understand roles, responsibilities and required skills when installing network cabling: • responsibilities: o install, terminate, test and certify cable (copper and fibre) o maintain cabling o identify, locate and repair faults o install cabinets, fixtures and racks o install physical protection measures for cabling o carry out risk assessments o work to relevant legislation o design and document and use cable route maps, testing and acceptance documentation o update asset registers o update maintenance logs o ensure system availability and performance

	• roles:
	  ○ cabling installer
	  ○ network surveyor
	  ○ network analyst
	  ○ network installation engineer
	• skills:
	  ○ manual handling
	  ○ working at height
	  ○ ability to interpret and follow plans
	  ○ adaptability
	  ○ prioritise tasks
	  ○ team working
	  ○ importance of upskilling.

5.5.3	Understand roles, responsibilities and required skills when providing digital support:
	• responsibilities:
	  ○ provide digital hardware support
	  ○ provide software support
	  ○ installation of software
	  ○ manage user accounts including storage quota and file permissions
	  ○ communicate support updates and system changes to end user
	  ○ train end users
	  ○ maintain asset registers
	  ○ use incident response software
	  ○ escalate issues when needed
	  ○ work to relevant legislation
	  ○ update standard operating procedures
	  ○ ensure system availability and performance
	• roles:
	  ○ first line support
	  ○ helpdesk/service desk
	  ○ support technician (desktop support, applications support, hardware support)
	• skills:
	  ○ problem solving
	  ○ analytical thinking
	  ○ use logging systems, monitoring and diagnostic tools
	  ○ communicate effectively
	  ○ prioritise tasks
	  ○ active listening
	  ○ customer service skills
	  ○ team working
	  ○ importance of upskilling.

5.5.4	Understand responsibilities when providing digital communications: • install, test and maintain integrated digital communication systems • manage availability of integrated digital communication systems • configure, monitor and optimise network performance for communication systems • apply security measures to integrated communication systems and networks • design and document systems to organisational standards.
5.5.5	Know the routes into digital support and security: • further education • apprenticeships • higher education • professional courses • professional recognition.

5.5.6	Understand communication techniques used in digital support and security:
	• incident tickets
	• system update notifications
	• forums
	• importance of clear, concise language based on audience needs:
	  ○ target audience
	  ○ audience size
	  ○ level of knowledge
	  ○ level of detail required
	• techniques:
	  ○ troubleshooting
	  ○ active listening
	  ○ reading of body language and body language factor
	  ○ expressions
	  ○ use of open questioning
	  ○ negotiation
	  ○ conflict handling/de-escalation.

5.5.7	Understand the interaction needs of end-users:
	• clients/end-users
	  ○ verbal support (in-person/over the phone/digital conference)
	  ○ written updates (email/support ticket system/IM)
	  ○ training (individual/classroom and pre-created e-learning)
	  ○ remote support
	  ○ screen sharing

	• managers:
	  ○ direction, support and escalation routes (email/support ticket)
	  ○ progress reports (written and verbal)
	  ○ presentation on progress/proposals
	• peers/colleagues:
	  ○ sharing of best practice
	  ○ dissemination of knowledge
	  ○ training
	  ○ collaborative working.

Content area 6: Emerging issues	
6.1 Impact of digital technologies	

6.1.1	Understand how the increased reliance on digital systems impacts on:
	• organisational culture:
	  ○ changes in communication methods (face to face, email, video calls)
	  ○ increased productivity and availability expectations
	  ○ increase in staff monitoring
	  ○ new working practices (remote/hybrid/in-office working)
	  ○ automation of services including the use of artificial intelligence (AI)
	• society:
	  ○ loss of jobs
	  ○ shift in skill requirements
	  ○ reduction in human decision making and loss of empathy
	  ○ privacy (digital footprint, surveillance)
	  ○ changing behaviours (loss of social skills, digital identity)
	  ○ access to wider social networks (personal and professional)
	  ○ access to online services (government, commercial and entertainment)
	  ○ potential isolation (lack of skill, equipment, connectivity, resistance to change)
	  ○ improved access to information (professional and personal)
	  ○ increased use of AI, including generative AI (textual, graphical, video and audio)
	  ○ globalisation:
	  – access to global media sources.

6.1.2	Understand the importance of digital inclusion:
	• ensuring fair access to digital services:
	  ○ suitable technologies (hardware and software)
	  ○ connectivity
	  ○ conforming to codes of best practice
	  ○ public sector bodies' website and mobile applications accessibility regulations:
	  – key features and purpose.

6.1.3	Understand how end user characteristics affect the use of and inclusivity of digital systems:
	• age
	• skills:
	  ○ digital
	  ○ literacy
	• internal/external audience:
	• cultural issues, including bias in digital systems
	• additional needs:
	  ○ accessibility issues.

6.1.4	Know and understand the benefits of professional development: • increased industry and sector competence • increased employability potential and employment security • achieving access to knowledge of and adherence to industry standards.
6.2 Emerging technologies	

6.2.1	Understand how developments in technologies impact on organisations, individuals and society:
	• storage media:
	  ○ increased demand for storage
	• processing technologies:
	  ○ quantum computing
	• internet of things:
	  ○ edge computing
	  ○ network utilisation
	  ○ use within different contexts (industrial, smart city, domestic)
	• artificial intelligence:
	  ○ generative AI
	  ○ machine learning
	• extended reality:
	  ○ augmented reality
	  ○ virtual reality
	• open source software
	• blockchain
	• 3D printing
	• drones
	• environmental:
	  ○ consumption of rare metals
	  ○ energy to produce electronic systems
	  ○ environmental impact of disposal
	• autonomous machines:
	  ○ self-driving cars
	  ○ robotic assembly lines.

6.2.2	Understand the interrelationships between digital and emerging technologies and make judgements about their impacts on organisations, society and individuals in digital support and security.

Content area 7: Digital environments	
7.1 Hardware	
7.1.1	Understand the features and use of different types of physical computers: • personal computers • mobile devices (smartphones and tablets) • servers • embedded devices

7.1.2	Understand the features and use of different types of hardware devices:
	• input devices
	• output devices
	• processors:
	  ○ number of cores
	  ○ clock speed
	  ○ cache size
	  ○ mobile processors
	• main memory:
	  ○ RAM (Random access memory)
	  ○ ROM (Read-only Memory)
	• secondary storage:
	  ○ magnetic
	  ○ solid state
	  ○ optical
	  ○ RAID (1, 5 and 10)
	  ○ NAS
	  ○ SAN
	• motherboard:
	• graphics processing units
	• network interface devices:
	  ○ PCI (Peripheral Component Interconnect)
	  ○ USB (Universal Serial bus)
	• cooling:
	  ○ air cooling
	  ○ liquid cooling
	• sensors.

7.2 Software	

7.2.1	Understand the features and use of operating systems:
	• batch:
	  ○ non-interactive applications
	  ○ high volume
	  ○ scheduling
	• multitasking:
	  ○ concurrent execution of multiple tasks
	  ○ time-slicing
	  ○ interrupts
	• real-time operating system:
	  ○ monitoring and control applications
	  ○ transaction processing
	• network operating system:
	  ○ resource sharing
	  ○ user management
	  ○ communication
	• mobile operating system:
	  ○ smartphones and tablets
	  ○ lower processing requirements
	  ○ increased battery life.

7.2.2	Understand the features and use of common utilities: • file management • defragmenters • file compression • package managers • protection software • backup software.
7.2.3	Understand the features and use of common application software: • word processors • spreadsheets • databases • email • project management software.

7.3 Networks	
7.3.1	Understand the benefits and drawbacks of connecting devices to form networks.

7.3.2	Know the different types of networks:
	• number of users
	• connection media
	• coverage area
	• network types:
	  ○ Personal Area Network (PAN)
	  ○ Local Area Network (LAN)
	  ○ Metropolitan Area Network (MAN)
	  ○ Wide Area Network (WAN).

7.3.3	Understand the features, characteristics, benefits and drawbacks of connectivity methods:
	• wired:
	  ○ copper/ethernet
	  ○ fibre-optic
	• wireless:
	  ○ wireless access points.

7.3.4	Understand the features, benefits and drawbacks of the common network topologies: • star • mesh • tree • logical versus physical.
7.3.5	Understand the features, benefits and drawbacks of different network models: • client-server • thin client • peer-to-peer.
7.3.6	Understand the role of common components of a network: • server • client • router • network switch • internet connection/internet backbone.

7.3.7	Understand the seven-layer OSI (open systems interconnection) model, including the function and related protocols of each layer: • application layer • presentation layer • session layer • transport layer • network layer • data link layer • physical layer.
7.3.8	Understand the four-layer TCP/IP (transmission control protocol/internet protocol) model, including the function and related protocols of each layer: • application layer • transport layer • internet layer • network layer.

7.3.9	Understand the role of data packets in transmitting over a network, including:
	• contents and structure of a data packet
	• role of the components of a data packet
	• packet switching:
	  ○ causes of packet loss
	• error handling:
	  ○ cyclic redundancy check (CRC).

7.3.10	Understand the role of common network protocols:
	• web protocols:
	  ○ HTTP
	  ○ HTTPS
	• mail protocols:
	  ○ SMTP
	  ○ POP
	  ○ IMAP
	• routing protocols:
	  ○ RIP
	  ○ OSPF
	• application protocols:
	  ○ FTP
	  ○ SFTP
	  ○ DHCP
	  ○ DNS.

7.3.11	Understand the concepts of bandwidth and latency, and their effect on the performance of networks and connected systems.

7.4 Virtual environments	

7.4.1	Understand the role and characteristics of common virtual environment components:
	• virtual machines:
	  ○ clients (virtual PC, virtual switch, virtual router)
	  ○ servers
	• hypervisors:
	  ○ type 1
	  ○ type 2.

7.4.2	Understand the key features of virtual environments: • increased security • managed execution • sharing • aggregation • emulation • isolation • portability.
7.4.3	Understand the benefits of the use of virtual environments: • cost effectiveness for large environments • easy management • resilience • potentially lower carbon footprint • improved disaster recovery options • better testing environments • provision of education and training options.
7.4.4	Understand the drawbacks of the use of virtual environments: • extra hardware load • slower execution time • potential for false representation of performance**.**
7.5 Cloud environments	
7.5.1	Understand different types of cloud: • private • public.
7.5.2	Understand the benefits of the use of cloud: • portability • elasticity • less storage limitations • cost effectiveness.

7.5.3	Understand common cloud delivery models, their advantages and disadvantages, and the way in which responsibility and ownership of resources are distributed between the client and cloud provider:
	• Infrastructure as a Service (IaaS):
	  ○ client manages application software, system software (middleware and operating system), runtime, data and user accounts
	  ○ cloud provider manages virtualisation and hardware (servers, network and storage)
	• Platform as a Service (PaaS):
	  ○ client manages application software, data and user accounts
	  ○ cloud provider manages virtualisation, hardware (servers, network and storage) and systems software (middleware and operating system) and runtime
	• Software as a Service (SaaS):
	  ○ client manages user accounts and data
	  ○ cloud provider manages virtualisation, hardware (servers, network and storage) systems software (middleware and operating system), runtime and application software.

7.6 Resilient digital environments	

7.6.1	Understand the benefits of resilient environments and the impact on organisations and clients:
	• increased security:
	  ○ data security (storage and transfer)
	  ○ reduce vulnerabilities
	• increased reputation:
	  ○ protect brand/image
	  ○ retain customer confidence
	• reduction in downtime.

7.6.2	Understand methods used to improve the resilience of digital environments:
	• software updates/upgrades:
	  ○ planned updates/upgrades
	  ○ patches in response to new vulnerabilities
	• hardware replacement:
	  ○ rolling replacement plans
	  ○ secure disposal
	• data and system redundancy
	• device hardening:
	  ○ removal of unneeded ports, applications, permissions and access
	• backup systems and recovery procedures:
	  ○ onsite
	  ○ remote/offsite
	  ○ cloud
	• hot, cold and warm sites

	• standard operating procedures:
	  ○ effective staff training
	  ○ induction
	  ○ new digital systems
	  ○ new or updated policies.

Content area 8: Security	
8.1 Security risks	

8.1.1	Know the type of confidential information held by organisations:
	• Human Resources:
	  ○ salaries and benefits
	  ○ staff personal details
	• commercially sensitive information:
	  ○ client details
	  ○ stakeholder details
	  ○ intellectual property
	  ○ sales numbers
	  ○ contracts
	• access information:
	  ○ usernames
	  ○ passwords
	  ○ multi-factor authentication details
	  ○ personal identification number (PIN)
	  ○ access codes
	  ○ passphrases
	  ○ biometric data.

8.1.2	Understand why information must be kept confidential by organisations:
	• salary and benefits:
	  ○ prevent competitors from offering higher wages to attract staff
	  ○ prevent employees from comparing salaries/demanding comparable pay
	• staff details:
	  ○ protect privacy
	  ○ prevent competitors from directly contacting them
	• intellectual property:
	  ○ prevent competitors from copying designs
	• client details:
	  ○ prevent competitors from contacting clients
	  ○ protect client privacy
	• sales numbers
	• access information:
	  ○ prevent unauthorised access.

8.1.3	Understand the potential impact to an organisation of failing to maintain privacy and confidentiality:
	• non-compliance with regulations:
	  ○ loss of licence to practice
	• loss of trust
	• damage to organisation's image
	• financial loss:
	  ○ fines
	  ○ refunds
	  ○ loss of earnings/termination of contracts
	• legal action
	• reduced security.

8.2 Types of threats and vulnerabilities	

8.2.1	Understand potential technical threats and their impacts on organisations and individuals, including prevention and mitigation methods:
	• botnets
	• denial of service (DoS)/Distributed Denial of Service (DDoS)
	• malicious hacking:
	  ○ hacktivists/nation states/organised crime/individual
	  ○ password cracking/brute force
	  ○ cross-site scripting
	  ○ SQL injection
	  ○ buffer overflow
	• malware:
	  ○ viruses
	  ○ worms
	  ○ key loggers
	  ○ ransomware
	  ○ spyware
	  ○ remote access trojans
	• social engineering:
	  ○ phishing
	  ○ spear phishing
	  ○ smishing
	  ○ vishing
	  ○ pharming
	  ○ watering hole attacks
	  ○ USB baiting
	• domain name server attack/redirection of traffic
	• open/unsecured Wi-Fi networks.

8.2.2	Understand potential technical vulnerabilities to systems and data:
	• inadequate security processes:
	  ○ weak encryption
	  ○ inadequate password policy
	  ○ failure to use multi-factor authentication
	• out-of-date components:
	  ○ hardware
	  ○ software (lack of support/compatibility with legacy systems, zero-day bugs)
	  ○ firmware.

8.2.3	Understand potential human threats, including prevention and mitigation methods, to systems and data:
	• human error:
	  ○ file properties
	  ○ confirmation boxes
	  ○ staff training
	• malicious employee:
	  ○ immediate removal from the premises
	  ○ suspend user accounts immediately
	• disguised criminal:
	  ○ accompany all visitors
	  ○ check identification of visitors
	• poor cyber hygiene:
	  ○ locking all unattended machines
	  ○ not writing passwords down
	  ○ poor password management.

8.2.4	Understand potential physical vulnerabilities, including prevention and mitigation methods, to systems, data and information, including:
	• lack of access control:
	  ○ entry control systems
	• poor access control:
	  ○ do not allow tailgating
	  ○ use complex access codes
	  ○ change codes regularly
	  ○ monitor access areas
	  ○ audit of staff access to secure areas
	• nature of location:
	  ○ protect against shoulder surfing
	  ○ protect against the environment
	  ○ protect against vandalism
	• poor system robustness:
	  ○ rugged machines
	• natural disasters.

8.2.5	Understand the potential impact to an organisation of threats and vulnerabilities: • loss/leaking of sensitive data • unauthorised access to digital systems • data corruption • disruption of service • unauthorised access to restricted physical areas.
8.3 Threat Mitigation	

8.3.1	Understand the purposes, processes, benefits and drawbacks of common threat mitigation techniques:
	• security settings:
	  ○ hardware
	  ○ software
	• anti-malware software:
	  ○ function
	  ○ actions
	• intrusion detection
	• encryption:
	  ○ hashing
	  ○ symmetric
	  ○ asymmetric
	• user access policies
	• staff vetting
	• staff training
	• software-based access control
	• device hardening
	• backups:
	  ○ type (full, incremental, differential)
	  ○ safe storage
	• software updates
	• firmware/driver updates
	• air gaps
	• certification of APIs (application programme interface)
	• VPNs (Virtual private networks)
	• multi-factor authentication (MFA)
	• password managers
	• port scanning
	• penetration testing:
	  ○ ethical hacking
	  ○ unethical hacking

8.3.2	Understand the processes and procedures that assure internet security, and the reasons why they are used:
	• firewall configuration:
	  ○ rules for traffic (inbound and outbound)
	  ○ traffic type rules
	  ○ application rules
	  ○ IP address rules
	• network segregation:
	  ○ virtual
	  ○ physical
	  ○ offline network
	• network monitoring
	• port scanning.

8.4 Interrelationship of components required for effective security	

8.4.1	Understand how the relationships in the CIA triad interrelate:
	• confidentiality:
	  ○ ensuring that data is kept private by controlling who has access to the data
	• integrity:
	  ○ ensuring that the data has not been tampered with; this can be done by maintaining confidentiality
	• availability:
	  ○ ensuring that data is available and useful; this can be done by ensuring integrity.

8.4.2	Understand the elements of the Identification Authentication Authorisation Accountability (IAAA) model, including the techniques used and their benefits and drawbacks:
	• identification:
	  ○ recognising the individual within a digital system
	  ○ knowledge-based identification, including username
	  ○ possession-based identification methods
	  ○ biometric-based ID methods
	• authentication:
	  ○ verifying the identity claimed during the identification phase
	  ○ multi-factor authentication methods
	  ○ passwords and pass phrases
	  ○ biometric authentication
	• authorisation:
	  ○ ensuring that authenticated users can only access resources and perform actions that they are permitted to
	  ○ role-based using the role of the user within the digital system
	  ○ access control lists

	• accountability:
	  ○ ensuring that any actions within a system can be traced back to the responsible user
	  ○ audit logs
	  ○ user activity monitoring.

Digital Infrastructure & Network Cabling Employer Set Project

Pre-task – Familiarisation with the industry context E1 E4 E6 M1 M2 M7 D1 D3 D5

The purpose of the pre-release task is to allow students the opportunity to familiarise themselves with the context of the main brief, i.e. the use of digital solutions in the financial sector.

Students are encouraged to carry out independent investigation and share findings with others, work in groups and communicate with others, and take part in and lead discussions.

Whilst the pre-release task is not directly assessed and not taken under controlled conditions, students will be able to use your research to inform responses to the assessed tasks.

Task 1 – Planning a project

Project planning tools

Be able to use project planning tools to apply understanding of project planning in response to a scenario.

Make use of given template (provided by Pearson) to produce a project plan containing a Gantt chart and a Resource and cost plan.

Gantt chart E4 E5 M1 M2 M3 M5 M8 M9 M10 D1 D2 D4

- Assess the strengths and skills of people and assign appropriate tasks to them.
- Make scheduling decisions in response to a defined deadline.
- Prioritise activities or tasks based on analysis of requirements.
- Demonstrate how to correctly and appropriately assign resources to project tasks.
- Use an appropriate project management methodology to efficiently organise project tasks.

Resource and cost plan E1 E4 M1 M2 M4 M8 D1 D2 D4

- Identify and calculate costs of a project, including:
  - materials
  - physical resources
  - personnel.
- Select and allocate resources to the resource list, and correctly attribute costs to provide an accurate estimate of the total project cost.
- Determine the affordability and viability of a implementing a project and its impact on a company over time.

Rationale E2 E3 E4 E5

- Consider the factors that are most relevant when planning projects.
- Justify notable project planning decisions made (particularly those that will have significant impact on the outcomes of the project), with consideration given to:
  - order and timing of tasks
  - allocation of team members
  - potential benefits and risks
  - impact of decisions on timings and costs.

Task 2 – Identifying and fixing defects in a network

Respond to a network simulation stimulus (provided as a Cisco Packet Tracer File).

Use of testing to identify defects

- Assess the given network/system against requirements.
- Carry out testing to identify issues in the network and associated devices.
- Perform any remedial actions required, justifying any decision made when fixing the defect.

Documenting the testing process E1 E4 M4 M8 D1 D2 D4

Provide annotated evidence of testing, including:

- identifying tests to be carried out
- describing the purpose of the identified test
- identifying test data or tool to be used (e.g. ping, tracer, specific IP addresses)
- describing the expected results
- describing the actual results of the tests performed
- comparing the actual results of testing with the expected results
- describing any further actions that are required
- refining the network/system as required.

The solution M4 M5 M7 D2 D4 D6

- Correct errors to ensure that the given network/system is functional and meets the given requirements.
- Follow appropriate conventions/procedures to ensure that the network/system produces consistently correct outcomes.

Task 3 – Designing a network solution

Produce a design for a network solution that meets identified needs

- Communicating the design through appropriate use of:
  - network diagram
  - annotations and/or additional information/descriptions.

Decomposition of the problem E1 E2 E3 E4 E5 M1 M5 M6 D1 D2 D4

- Break down the problem into smaller parts suitable for network/hardware-based solutions – identifying the required hardware, software, settings and data connections.
- Grouping tasks/requirements to groups of users.
- Identifying specific tools and components for tasks/users.
- Use elements of reusable components (e.g. group permissions, virtual/physical components).
- Use good decomposition to show all the necessary parts that make up the main solution.

Application of logical thinking M1 D2

- Describe the parts of the solution (e.g. IP schemes, computer names, routing etc).
- Application of good network design principles (e.g. appropriate topologies, network segmentation, security, redundancy).
- Correct logic when configuring systems (e.g. authentication, permissions, sub netting).

Use of conventions E3 M4

- Demonstrate correct use of structure and convention for the chosen method of communication (Network diagram, annotations/additional information), such as correct use of IP address masks, identifiable network components/symbols.
- Select and make consistent use of appropriate entity names.

Communication of the design E4 M1 D4

- Ensure design documents are of sufficient detail to:
  - effectively communicate the intended solution
  - allow the client to make informed decisions
  - allow a third party to use design documents to create the proposed solution.
- Communicate intended solution effectively and clearly, with use of:
  - appropriate combination of written and diagrammatical presentation
  - appropriate use of technical vocabulary
  - consideration of audience
  - explanations of structures and process in the design.

Task 4a – Developing a solution

The solution E1 E5 M2 M4 M5 M6 M7 D1 D4 D6

Apply an undertaking of network infrastructure to develop a solution that meets the requirements of a brief, including:

- refining and developing the given network simulation as required
- selecting appropriate tools, devices and settings to meet the requirements
- demonstrating an appropriate level of technical skill, and understanding of networks/hardware/software techniques and problem solving.

Robustness

Ensure the network produced provides adequate levels of robustness for users and the given scenario including:

- system resilience (e.g. user management, device/system hardening, segmentation)
- redundancy (e.g. back-up systems and procedures, fall backs, UPS).

Security M6

- Apply an understanding of network and system security including:
  - configuring security software (e.g. anti-malware, firewalls)
  - configuring user roles and network permissions
  - hardening and air-gapping.

Organisation M4

Ensure network produced for the solution is appropriate to meet the demands of the brief, including:

- use of networking knowledge including:
  - configuring servers
  - configuring and deploying nodes on the network
  - selection of appropriate connection media
  - selection and configuration of wired and wireless access to the network
  - network regions/subnets.
- knowledge of hardware/software including:
  - configuring nodes on a hardware level (e.g. building a PC that meets specific requirements)
  - installing and configuring software.

User experience E4

Meet user needs, with consideration and selection of:

- end user devices
- data connections
- back-end systems
- access and availability.

Task 4b – Reflective evaluation

Review of outcomes E1 E2 E3 E4 D3

- Be able to apply reflection and evaluation techniques.
- Provide evidence that the product meets brief requirements:
  - include measures against success criteria
  - provide evidence that the product meets user needs
  - discuss how it could be improved if the problem was revisited and given detailed consideration.

Cyber Security Employer Set Project

Pre-task – Familiarisation with the industry context E1 E4 E6 M1 M2 M7 D1 D3 D5

The purpose of the pre-release task is to allow students the opportunity to familiarise themselves with the context of the main brief, i.e. the use of digital solutions in the financial sector.

Students are encouraged to carry out independent investigation and share findings with others, work in groups and communicate with others, and take part in and lead discussions.

Whilst the pre-release task is not directly assessed and not taken under controlled conditions, students will be able to use your research to inform responses to the assessed tasks.

Task 1 – Planning a project

Project planning tools

Be able to use project planning tools to apply understanding of project planning in response to a scenario.

Make use of given template (provided by Pearson) to produce a project plan containing a Gantt chart and a resource and cost plan.

Gantt chart E4 E5 M1 M2 M3 M5 M8 M9 M10 D1 D2 D4

- Assess the strengths and skills of people and assign appropriate tasks to them.
- Make scheduling decisions in response to a defined deadline.
- Prioritise activities or tasks based on analysis of requirements.
- Demonstrate how to correctly and appropriately assign resources to project tasks.
- Use an appropriate project management methodology to efficiently organise project tasks.

Resource and cost plan E1 E4 M1 M2 M4 M8 D1 D2 D4

- Identify and calculate costs of a project, including:
  - materials
  - physical resources
  - personnel.
- Select and allocate resources to the resource list, and correctly attribute costs to provide an accurate estimate of the total project cost.
- Determine the affordability and viability of implementing a project and its impact on a company over time.

Rationale E2 E3 E4 E5

- Consider the factors that are most relevant when planning projects.
- Justify notable project planning decisions made (particularly those that will have significant impact on the outcomes of the project), with consideration given to:
  - order and timing of tasks
  - allocation of team members
  - potential benefits and risks
  - impact of decisions on timings and costs.

Task 2 – Identifying and fixing security defects

Respond to a network simulation stimulus (provided as a Cisco Packet Tracer File).

Use of testing to identify defects

- Assess the given network simulation against requirements.
- Carry out testing to identify issues in the network and associated devices.
- Perform any remedial actions required, justifying any decision made when fixing the defect.

Documenting the testing process E1 E4 M4 M8 D1 D2 D4

Provide annotated evidence of testing, including:

- identifying tests to be carried out
- describing the purpose of the identified test
- identifying test data or tool to be used (e.g. ping, tracer, specific IP addresses)
- describing the expected results
- describing the actual results of the tests performed
- comparing the actual results of testing with the expected results
- describing any further actions that are required
- refining the network/system and related security procedures as required.

The solution M4 M5 M7 D2 D4 D6

- Correct errors to ensure that the given network simulation is functional and meets the given requirements.
- Follow appropriate conventions/procedures to ensure that the network is secure.

Task 3 – Designing a solution

Produce a security plan that meets the needs of a given scenario

Decomposition of the problem E1 E2 E3 E4 E5 M1 M5 M6 D1 D2 D4

- Break down the problem into smaller parts appropriate for application of a cyber security solution, identifying the relevant physical, logical/software, and user-based risks.
- Identify specific issues with different areas of the network and/or people.
- Use good decomposition to show all the issues that would need to be mitigated to ensure the network is secure.

Application of security measures and conventions M1 D2

- Describe how identified risks could be mitigated.
- Application of accepted cyber security good practice.
- Use of multiple security measures and fail safes to guard against a range of potential attack vectors and mitigate failure of a single line of defence.
- Using industry standard tools and procedures to mitigate risks and protect systems.

Communication of the design E4 M1 D4

- Ensure design documents are of sufficient detail to:
  - effectively communicate the intended solution
  - allow the client to make informed decisions
  - allow a third party to use design documents to create the proposed solution.
- Communicate intended solution effectively and clearly, with use of:
  - appropriate use of technical vocabulary
  - consideration of audience
  - explanations of structures and process in the design.

Task 4a – Developing a solution

The solution E1 E5 M2 M4 M5 M6 M7 D1 D4 D6

Apply an undertaking of cyber security to develop a secure solution that meets the requirements of a brief, including:

- refining and developing the given network simulation as required
- selecting appropriate tools, devices and settings to meet the requirements
- demonstrating an appropriate level of technical skill and understanding of networks/hardware/software techniques and problem solving.

Techniques and considerations

Ensure the network produced provides adequate levels of security and robustness for users and the given scenario including:

- system resilience (e.g. user management, device/system hardening, segmentation)
- redundancy (e.g. back-up systems and procedures, fall backs, UPS).

Vulnerabilities M6

Application of network and system security to mitigate against potential vulnerabilities including:

- configuring security software (e.g. anti-malware, firewalls)
- configuring user roles and network permissions
- hardening and air-gapping.

Solution organisation M4

Ensure network produced for the solution is appropriate to meet the demands of the brief, including:

- Use of networking knowledge including:
  - configuring servers
  - configuring and deploying nodes on the network
  - selection of appropriate connection media
  - selection and configuration of wired and wireless access to the network
  - network regions/subnets
  - providing potential for future scalability while maintaining security.
- Knowledge of hardware/software including:
  - configuring nodes on a hardware level (e.g. building a PC that meets specific requirements)
  - installing and configuring software.

Task 4b – Reflective evaluation E1 E2 E3 E4 D3

Review of outcomes

- Be able to apply reflection and evaluation techniques.
- Provide evidence that the product meets brief requirements:
  - include measures against success criteria
  - provide evidence that the product meets user needs
  - discuss how it could be improved if the problem was revisited and given detailed consideration.

Digital Support Technician Employer Set Project

Pre-task – Familiarisation with the industry context E1 E4 E6 M1 M2 M7 D1 D3 D5

The purpose of the pre-release task is to allow students the opportunity to familiarise themselves with the context of the main brief, i.e. the use of digital solutions in the financial sector.

Students are encouraged to carry out independent investigation and share findings with others, work in groups and communicate with others, and take part in and lead discussions.

Whilst the pre-release task is not directly assessed and not taken under controlled conditions, students will be able to use your research to inform responses to the assessed tasks.

Task 1 – Planning a project

Project-planning tools

Be able to use project-planning tools to apply understanding of project planning in response to a scenario.

Make use of given template (provided by Pearson) to produce a project plan containing a Gantt chart and a Resource and cost plan.

Gantt chart E4 E5 M1 M2 M3 M5 M8 M9 M10 D1 D2 D4

- Assess the strengths and skills of people and assign appropriate tasks to them.
- Make scheduling decisions in response to a defined deadline.
- Prioritise activities or tasks based on analysis of requirements.
- Demonstrate how to correctly and appropriately assign resources to project tasks.
- Use an appropriate project management methodology to efficiently organise project tasks.

Resource and cost plan E1 E4 M1 M2 M4 M8 D1 D2 D4

- Identify and calculate costs of a project, including:
  - materials
  - physical resources
  - personnel.
- Select and allocate resources to the resource list, and correctly attribute costs to provide an accurate estimate of the total project cost.
- Determine the affordability and viability of a implementing a project and its impact on a company over time.

Rationale E2 E3 E4 E5

- Consider the factors that are most relevant when planning projects.
- Justify notable project planning decisions made (particularly those that will have significant impact on the outcomes of the project), with consideration given to:
  - order and timing of tasks
  - allocation of team members
  - potential benefits and risks
  - impact of decisions on timings and costs.

Task 2 – Diagnosing issues and providing support

Respond to a set of prompts/support tickets and a simulation stimulus (provided as a Cisco Packet Tracer File).

Use of testing to identify defects

- Assess the support tickets.
- Apply and understating of testing and root cause analysis to identify potential causes and suggest a range of possible solutions.
- Assess the simulated issues.
- Carry out testing to identify the cause of the issues in the network and/or associated devices.
- Perform any remedial actions required, justifying any decision made when fixing the defect.

Communicating the process E1 E4 M4 M8 D1 D2 D4

- Identify potential causes for the issue raised by the support ticket.
- Describe potential solutions that could be implemented.

The solution M4 M5 M7 D2 D4 D6

Provide annotated evidence of testing, including:

- identifying tests to be carried out
- describing the purpose of the identified test
- identifying test data or tool to be used (e.g. ping, tracer, specific IP addresses)
- describing the expected results
- describing the actual results of the tests performed
- comparing the actual results of testing with the expected results
- describing any further actions that are required
- refining the network/system as required
- performing actions to fix the identified issue to ensure the simulated solutions work as expected.

Task 3 – Planning a solution

Carry out a needs analysis and show how digital technologies could be implemented to meet the requirements of a given organisation.

Decomposition of the problem E1 E2 E3 E4 E5 M1 M5 M6 D1 D2 D4

- Apply an understating of decomposition to break down the situation down into smaller parts.
- Use decomposition to ensure coverage of a wide range of suitable of general and specific needs of the organisation and its stakeholders.
- Provide a detailed description of the hardware, software and data communication technologies that should be implemented to meet the identified requirements.

Risk mitigation M1 M4 D2

- Assesses the potential risks to the organisation and its systems.
- Suggest a range of measures that can be employed to mitigate the identified risks.

Communication of the solution E4 M1 D4

- Ensure needs analysis is of sufficient detail to:
  - effectively communicate the intended solution
  - allow the client to make informed decisions
  - allow a third party to use documents to create the proposed solution.
- Communicate intended solution effectively and clearly, with use of:
  - appropriate combination of written and diagrammatical presentation
  - appropriate use of technical vocabulary
  - consideration of audience
  - explanations of processes and procedures to be implemented.

Task 4a – Developing a solution

The solution E1 E5 M2 M4 M5 M6 M7 D1 D4 D6

Apply an undertaking of digital support to develop a solution that meets the requirements of a brief, including:

- refining and developing the given network simulation as required
- selecting appropriate tools, devices and settings to meet the requirements
- demonstrating an appropriate level of technical skill and understanding of networks/hardware/software techniques and problem solving.

Robustness

Ensure the network produced provides adequate levels of robustness for users and the given scenario including:

- system resilience (e.g. user management, device/system hardening, segmentation)
- redundancy (e.g. back-up systems and procedures, fall backs, UPS).

Security M6

- Apply an understanding of network and system security including:
  - configuring security software (e.g. anti-malware, firewalls)
  - configuring user roles and network permissions
  - hardening and air-gapping.

Organisation M4

Ensure network produced for the solution is appropriate to meet the demands of the brief, including:

- use of networking knowledge including:
  - configuring servers
  - configuring and deploying nodes on the network
  - selection of appropriate connection media
  - selection and configuration of wired and wireless access to the network
  - network regions/subnets.
- knowledge of hardware/software including:
  - configuring nodes on a hardware level (e.g. building a pc that meets specific requirements)
  - installing and configuring software.

User experience E4

Meet user needs, with consideration and selection of:

- end user devices
- data connections
- back-end systems
- access and availability.

Task 4b – Reflective evaluation

Review of outcomes E1 E2 E3 E4 D3

- Be able to apply reflection and evaluation techniques.
- Provide evidence that the product meets brief requirements:
  - include measures against success criteria
  - provide evidence that the product meets user needs
  - discuss how it could be improved if the problem was revisited and given detailed consideration.

Scheme of Assessment – Core Component

There are three assessments in the Core component of the *T Level Technical Qualification in Digital Support and Security*:

- Core Examination Paper 1
- Core Examination Paper 2
- Employer Set Project.

The mapping, timings, scheduling and preparation for the assessments shown below are for the current specimen assessment material. The actual live assessments will have the same overarching number of tasks and overall focus. However, the order of tasks and the details within the task may change each series.

Core examination

Paper 1
Written examination: 2 hours 15 minutes **30% of the core assessments** **90 marks**
Content overview 1. Problem solving 2. Introduction to digital support 3. Data
Assessment overview A written examination comprising two sections, A and B Students answer all questions in each section. Each section of the examination will get more challenging as the student progresses by ramping up demand and difficulty in a manner broadly similar to the other sections. Each section will be assessed through a combination of: • short open response items • medium open response items • extended open response questions. The examination is: • set and marked by Pearson • timetabled at a time and on a date specified by Pearson.
Administration This paper must be assessed under examination conditions following JCQs Instructions for Conducting Examinations (ICE).

Paper 2
Written examination: 2 hours 15 minutes **30% of the core assessments** **90 marks**
Content overview 4. Legislation and regulatory requirements 5. Business context 6. Emerging issues 7. Digital environments 8. Security
Assessment overview A written examination comprising two sections, A and B. Students answer all questions in each section. Each section of the examination will get more challenging as the student progresses by ramping up demand and difficulty in a manner broadly similar to the other sections. Each section will be assessed through a combination of: • short open response items • medium open response items • extended open response questions. The examination is: • set and marked by Pearson • timetabled at a time and on a date specified by Pearson.
Administration This paper must be assessed under examination conditions following JCQs Instructions for Conducting Examinations (ICE).

Core Examination Assessment Objectives

Assessment Objective		Paper 1 (Marks/%)	Paper 2 (Marks/%)
AO1a	Demonstrate knowledge and understanding of the content (knowledge)	8 (8.9%)	10 (11.1%)
AO1b	Demonstrate knowledge and understanding of the content (understanding)	22 (24.4%)	21 (23.3%)
AO2	Apply knowledge and understanding of the content to different situations and contexts	39 (43.3%)	38 (42.2%)
AO3a	Analyse information and issues related to the content	12 (13.3%)	12 (13.3%)
AO3b	Evaluate information and issues related to the content	9 (10%)	9 (10%)

Paper 1	AO1a	AO1b	AO2	AO3a	AO3b
Section A	8	16	3	3	0
Section B	0	6	36	9	9
Total 90 marks	30		39	21	

Paper 2	AO1a	AO1b	AO2	AO3a	AO3b
Section A	6	18	3	3	0
Section B	4	3	35	9	9
Total 90 marks	31		38	21	

Employer Set Project

Employer Set Project
Externally assessed project: 14 hours 30 minutes **40% of the core assessments** **Total marks 89-100**
Content overview When responding to the Employer Set Project, students will need to draw upon knowledge and skills from across the Core content in a synoptic manner to effectively respond to a brief within a vocational context.
Assessment overview There is a pre-release task that is not assessed. There are five parts to the assessment: • Task 1: Planning a project • Task 2: Identifying and fixing defects in a given digital system • Task 3: Designing/Planning a solution • Task 4a: Developing a solution • Task 4b: Reflective evaluation Students will undertake the assessed elements of the project tasks under supervised conditions. Internet access is not permitted. Students may not use AI or any other tool designed to prepare a response. The assessment will take place over multiple sessions up to a combined duration of 14 hours 30 minutes. The project outcomes will consist of a portfolio of evidence submitted electronically. Students will undertake a project in response to a realistic contextual challenge. The project is validated by an employer panel, taking into account the client's requirements and the user experience. The project will consist of planning documentation, an annotated digital portfolio, prototype digital product, testing evidence and evaluation. The project will be set and marked by Pearson.
Administration Providers must follow the guidance in the following: • General Administrative Support Guide • Administration Support Guide for the specific Technical Qualification Employer Set Project (if applicable). These are located on the Training and Admin Support webpage.

Employer Set Project Assessment Objectives

The Digital Support and Digital Infrastructure and Network Cabling ESPs have targeted weightings to AOs as shown in the table below:

Assessment Objective			Proportion
AO1	**Planning**	Plan an approach to developing solutions to solve problems in response to a brief.	12%
AO2	**Application**	Apply knowledge and skills to develop software, create an artefact, fix defects and mitigate risks to security.	41%
AO3	**Selecting relevant techniques and resources**	Select relevant tools, techniques and resources to respond to a brief and work in a collaborative environment.	9%
AO4	**a. English skills**	Use appropriate English skills to communicate technical information to both technical and non-technical audiences.	3%
	b. Maths skills	Use appropriate maths skills to realise a project outcome in response to a brief.	
	c. Digital skills	Use appropriate digital skills to realise a project outcome in response to a brief and communicate technical information to both technical and non-technical audiences.	
AO5	**d. Project outcome**	Realise a project outcome by producing software and artefacts in response to a brief.	26%
	e. Review	Review how well digital solutions meet a brief, using reflective evaluation.	9%

The Cyber Security ESP has targeted weightings to AOs as shown in the table below:

Assessment Objective			Proportion
AO1	**Planning**	Plan an approach to developing solutions to solve problems in response to a brief.	13.5%
AO2	**Application**	Apply knowledge and skills to develop software, create an artefact, fix defects and mitigate risks to security.	49.4%
AO3	**Selecting relevant techniques and resources**	Select relevant tools, techniques and resources to respond to a brief and work in a collaborative environment.	10.1%
AO4	**a. English skills**	Use appropriate English skills to communicate technical information to both technical and non-technical audiences.	3.4%
	b. Maths skills	Use appropriate maths skills to realise a project outcome in response to a brief.	
	c. Digital skills	Use appropriate digital skills to realise a project outcome in response to a brief and communicate technical information to both technical and non-technical audiences.	
AO5	**d. Project outcome**	Realise a project outcome by producing software and artefacts in response to a brief.	13.5%
	e. Review	Review how well digital solutions meet a brief using reflective evaluation.	10.1%

Resources for the delivery of the Core component content

Providers must ensure that the student has access to the necessary materials, resources and workspaces for delivery and assessment:

- word processing (for example, MS Word, Google Docs)
- presentation (for example, MS PowerPoint, Google Slides)
- spreadsheet (for example, MS Excel, Google Sheets)
- diagramming software with suitable features and tools for creating network diagrams.
- project management (for example, MS Excel, MS Project)
- basic image editing software (for example, Adobe Photoshop, GIMP)
- programming software
- database software (for example, MS SQL, MySQL)
- web browsers
- Cisco packet tracer or any alternatives that can load a .pkt file/

Students should also be given the opportunity to experience physical networking tasks so will need access to:

- physical devices (mobile devices, PCs/laptops, servers) – note that hardware needs to be able to run the required software)
- connection media (e.g. ethernet cables)
- networking devices (e.g. access points, switches, routers)
- access to a range of data sources (for example online, social media, analytical)
- internet access
- access to a range of research resources (for example online, books, journals)
- hardware:
    - mobile devices
    - media to support installation and deployment of operating systems
    - access to appropriate network architecture devices (for example server, switch, hub, firewalls, load balancer).

4 Occupational Specialisms

1. Digital Infrastructure

Content area 1: Apply procedures and controls to maintain the digital security of an organisation and its data

What underpinning knowledge do students need?	

1.1	**Understand the role and types of preventative business control techniques and be able to apply and maintain them in protecting the digital security of an organisation**
	• Role – proactive control that stops something happening.
	• Preventative control techniques:
	  ○ physical:
	  – specialist locks (for example anti-picking)
	  – barriers (for example, fencing, bollards)
	  – gates
	  – cages
	  – flood defence systems
	  – temperature controls (for example, air conditioning)
	  ○ combined – managed access:
	  – card readers
	  – biometric
	  – video/closed-circuit television (CCTV)
	  – pin/passcodes
	  ○ administrative, policies and procedures:
	  – separation of duties and relevance of role-based access
	  ○ technical – domains and security policies:
	  – allowlist
	  – denylist
	  – access control lists
	  – sandboxing
	  – device hardening
	  – certificate authority.
	• Set up a domain services environment with security controls (for example, group policies, minimum password requirements).
	• Set up and deploy a certificate authority (for example, server deployment).

	• Implement security controls in a business environment in line with NCSC cyber essentials:
	  ○ boundary firewalls
	  ○ secure configuration (for example, enabling multi-factor authentication)
	  ○ access control
	  ○ malware protection
	  ○ patch management.
	• Configure and apply appropriate access control methods to physical or virtual networks (for example authentication, MAC, DAC, ABAC, RBAC).
	• Manage documents and data accurately in accordance with data protection legislation.
	(E5, D1, D5, D6)

1.2	**Understand the role and types of detective business control techniques in protecting the digital security of an organisation**
	• Role – to identify an incident in progress or retrospectively.
	• Detective control techniques:
	  ○ physical:
	  – CCTV
	  – motion sensors
	  ○ administrative, policies and procedures:
	  – logs (for example logs of temperature in server room, error logs)
	  – review/audit (for example people entering and leaving the facilities).

1.3	**Understand the role and types of corrective business control techniques in protecting the digital security of an organisation**
	• Role – reactive measures to limit the extent of damage and reoccurrence.
	• Corrective control techniques:
	  ○ physical:
	  – fire suppression (for example sprinklers, extinguishers)
	  – gas suppression (for example inert and chemical gas systems)
	  ○ administrative, policies and procedures:
	  – standard operating procedure (for example actions taken when a fire is identified).

1.4	**Understand the role and types of deterrent business control techniques in protecting the digital security of an organisation**
	• Role – pre-emptive measures to dissuade a course of action.
	• Deterrent control techniques:
	  ○ physical:
	  – security guards
	  – alarm systems
	  – visible surveillance systems

	○ administrative, policies and procedures: – standard operating procedure (for example setting alarm system, fire drill) – employment contracts stipulating codes of conduct – acceptable usage policies.
1.5	**Understand the role and types of directive business control techniques in protecting the digital security of an organisation** • Role – promotes a security-focused business culture. • Directive control techniques: ○ physical: – signage – mandatory ID badge display (for example employees and visitors) ○ administrative, policies and procedures: – agreement types – general security policies and procedures – regular and compulsory staff training (for example human firewall training).
1.6	**Understand the role and types of compensating business control techniques in protecting the digital security of an organisation** • Role – provides a safeguard against primary control failure • Compensating control techniques: ○ physical: – temperature controls (for example air conditioning) ○ administrative, policies and procedures: – role-based awareness training – standard operating procedures (for example environmental control monitoring).
1.7	**Be able to apply and monitor appropriate business control techniques and policies and procedures to ensure personal, physical and environmental security** • Review the identified risk: ○ gather information from system and users. • Select, apply and monitor appropriate business control techniques: ○ preventative ○ detective ○ corrective ○ deterrent ○ directive ○ compensating ○ recovery. • Comply with relevant regulatory and organisational policies and procedures. (D3)

1.8	**Understand the role and implementation of a disaster recovery plan in protecting the digital security of an organisation**
	• Role – to recover and maintain service.
	• Disaster recovery plan:
	  ○ physical:
	  – back-ups
	  – off-site alternative storage of servers
	  ○ administrative, policies and procedures of a disaster recovery plan (DRP) supported by an organisational business continuity plan (BCP):
	  – ensuring all systems maintain functionality (for example arranging hardware)
	  – ensuring users can access systems away from the main building site
	  – deploying back-ups to maintain data integrity
	  – ensuring digital changes continue to meet business needs
	  – managing assets across the network and logging changes (for example tagging and logging laptops)
	  – reporting infrastructure changes to management.

1.9	**Understand how a disaster recovery plan (DRP) works**
	• Define the scope of the plan:
	  ○ data centre premises
	  ○ organisational
	  ○ departmental
	  ○ individual.
	• Gathering relevant information:
	  ○ historic outage details
	  ○ inventories of hardware, software, networks and data
	  ○ contact information for any involved parties.
	• Risk-assessing:
	  ○ assets
	  ○ threats
	  ○ vulnerabilities
	  ○ probability of occurrence
	  ○ impact on business/data.
	• Creating the plan:
	  ○ identify the resources required for the DRP:
	  – systems
	  – equipment.
	• Plan approval:
	  ○ sign off by appropriate party.

	• Testing the plan:
	  ○ identify scope:
	  – identify resources
	  – determining frequency
	  – implement test
	  – review and document outcome
	  – amend the plan based on review as required
	  ○ continuous improvement:
	  – internal and external auditing of plan.

1.10	**Understand the types of impacts that can occur within an organisation as a result of threats and vulnerabilities** • Danger to life – breaches in health and safety policies (for example injury and death). • Privacy – breaches of data (for example compromised confidential business data, identity theft). • Property and resources – damage to property and systems. • Economic – financial loss or impairment. • Reputation – damage to brand and business value. • Legal – fines or prosecution.

1.11	**Understand the potential vulnerabilities in critical systems**
	• Unauthorised access to network infrastructure.
	• Unauthorised physical access to network ports.
	• Single point of failure.
	• System failure.
	• Open port access:
	  ○ USB (universal serial bus)
	  ○ wireless networks.

1.12	**Understand the impact of measures and procedures that are put in place to mitigate threats and vulnerabilities**
	• Measures:
	  ○ recovery time objective (RTO)
	  ○ recovery point objective (RPO)
	  ○ mean time between failure (MTBF)
	  ○ mean time to repair (MTTR).
	• Procedures:
	  ○ standard operating procedure (SOP):
	  – installation procedure
	  – back-up procedure
	  – set-up procedure
	  ○ service level agreement (SLA):
	  – system availability and uptime
	  – response time and resolution timescales.

1.13	**Understand the process of risk management**
	• Process:
	  ○ identification – identifying potential risks, threats or vulnerabilities
	  ○ probability – likelihood of occurrence (for example high, medium, low)
	  ○ impact – assess damage that can occur (for example asset value)
	  ○ prioritisation – rank risks based on the analysis of probability and impact, ownership of risk
	  ○ mitigation – reducing probability or impact of risk.

1.14	**Understand approaches and tools for the analysis of threats and vulnerabilities**
	• Approaches:
	  ○ qualitative – non-numeric:
	  – determine severity using red, amber, green (RAG) rating:
	  – red – high risk requiring immediate action
	  – amber – moderate risk that needs to be observed closely
	  – green – low risk with no immediate action required
	  ○ quantitative – numeric:
	  – analyse effects of risk (for example cost overrun, resource consumption).
	• Tools:
	  ○ fault tree analysis
	  ○ impact analysis
	  ○ failure mode effect critical analysis
	  ○ annualised loss expectancy (ALE)
	  ○ Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)
	  ○ strength, weakness, opportunity, threat (SWOT) analysis
	  ○ risk register – risk is identified and recorded using a RAG rating.

1.15	**Understand factors involved in threat assessment for the mitigation of threats and vulnerabilities**
	• Environmental:
	  ○ extreme weather
	  ○ natural disaster
	  ○ animals (for example rodent in server room)
	  ○ humidity
	  ○ air quality.
	• Manmade:
	  ○ internal:
	  – malicious or inadvertent activity from employees and contractors

	○ external: – malware – hacking – social engineering – third-party organisations – terrorism. • Technological: ○ technology failures and faults: – misconfigured devices – disk failure/corruption – component failure – power issues – network dropouts – inaccessible systems – virtual private network (VPN) not connecting – unresponsive systems – device failures and faults (for example laptops, desktops, servers) – hard disk failure – random access memory (RAM) failure – damaged peripherals – device incorrectly configured – additional card implementation (for example network interface card (NIC), graphics) – server back-up set-up. • System failures and faults: ○ firewall settings ○ software breakages/corruption ○ redundant array of independent disks (RAID) failure. • Impact of technical change: ○ potential downtime ○ requirement for system or software upgrades ○ misconfigured systems. • Political: ○ changes or amendments in legislation.
1.16	**Understand the purpose of and be able to carry out risk assessment in a digital infrastructure context** • Purpose: ○ to identify and reduce risk by: – implementing Health and Safety Executive (HSE) guidelines to projects (for example installing a new uninterruptible power supply (UPS) system into a server room and identifying risks to the installers) – investigating risks within the project environment (for example undertaking a PESTLE analysis)

	– internal and external risk identification (for example implementing a supply chain assessment) – quantification of impact on asset value (for example financial loss as a result of downtime). • Conduct a security risk assessment in line with the risk management process for a system (for example a device connected to a local area network LAN): o assess the system and identify components o apply the risk management process: – identify possible risks within the system – calculate the probability and impact of the identified risk – analyse and prioritise based on level of risk to system o record all relevant findings and actions accurately and concisely using appropriate technical terms. (E4, M6, D4)
1.17	**Understand types of risk response within a digital infrastructure context** • Types of response: o accept – the impact of the risk is deemed acceptable o avoid – change scope to avoid identified risk o mitigate – reduce the impact or probability of the identified risk o transfer – contractually outsource the risk to another party.
1.18	**Understand the process of penetration testing within digital infrastructure** • Penetration testing (for example wireless network tests): o customer engagement o information gathering o discovery and scanning o vulnerability testing o exploitation o final analysis and review o utilise the test results.
1.19	**Understand the considerations in the design of a risk mitigation strategy** • Risk response (for example, accept, avoid, mitigate or transfer the risk). • User profile (for example, requirements, ability level). • Cost and benefit. • Assign an owner of the risk. • Escalation to appropriate authority within organisation. • Planning contingencies. • Monitoring and reviewing process.

1.20	**Understand the purpose of technical security controls as risk mitigation techniques and their applications to business risks within a digital infrastructure context**
	• Purpose – to improve network security for users and systems.
	• Technical security controls and their applications:
	  ○ 5 cyber essentials controls:
	  – boundary firewalls and internet gateways – restricting the flow of traffic in systems
	  – secure configuration – ensuring user only has required functionality (for example, removing unnecessary software, configuration to limit web access)
	  – malware protection – maintaining up-to-date anti-malware software and regular scanning
	  – patch management – maintaining system and software updates to current levels
	  – access control – restricting access to a minimum based on user attributes (for example principle of least privilege, username and password management)
	  ○ device hardening – removing unneeded programs, accounts functions, applications, ports, permissions and access
	  ○ segmentation – network, systems, data, devices and services are split up to mitigate the potential impact of risks
	  ○ hardware protection – using server and software solutions to protect hardware and data
	  ○ multi-factor authentication – allowing 2 devices to authenticate against one system to confirm who and where the user is trying to access from
	  ○ remote monitoring and management (RMM) (for example, end user devices)
	  ○ vulnerability scanning (for example, port scanning, device scanning).

1.21	**Be able to demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a digital infrastructure context**
	• Identify, gather and systematically organise information on incidents in preparation for analysis.
	• Process and analyse trends in incident data to identify underlying risks, identify user profile (for example, requirements, ability level).
	• Identify and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in end user devices (for example installing RMM software, device hardening).
	• Monitor and review as part of a continuous improvement process:
	  ○ assign an owner of the risk
	  ○ plan contingencies
	  ○ update devices with current security software
	  ○ interpret the outputs of penetration testing.

	• Record all relevant findings and actions accurately and concisely using appropriate technical terms. (E4, M5, D4)

1.22	**Understand the purpose and types of encryption as a risk mitigation technique and their applications**
	• Purpose – to store and transfer data securely using cryptography.
	• Types of encryption and their applications:
	  ○ asymmetric encryption – applied to send private data from one user to another (for example encrypted email systems)
	  ○ symmetric encryption – applied to encrypt and decrypt a message using the same key (for example card payment systems)
	  ○ data at rest encryption:
	  – full disk encryption – applied to encrypt the contents of an entire hard drive using industry standard tool (for example Windows, macOS)
	  – hardware security module (HSM) – safeguards digital keys to protect a device and its data from hacking
	  – trusted platform module (TPM) – applied to store encryption keys specific to the host device
	  ○ data in transit encryption:
	  – secure sockets layer (SSL) – applied to create an encrypted link between a website and a browser using security keys for businesses to protect the data on their websites
	  – transport layer security (TLS) – applied to encrypt end-to-end communication between networks (for example in email, websites and instant messaging).

1.23	**Understand the purpose, criteria and types of back-up involved in risk mitigation**
	• Purpose:
	  ○ maintaining an up-to-date copy of data to enable future recovery and restoration (for example full disaster recovery or partial data loss).
	• Back-up criteria:
	  ○ frequency (for example periodic back-ups)
	  ○ source (for example files or data)
	  ○ destination (for example internal, external)
	  ○ storage (for example linear tape open (LTO), cloud, disk).
	• Types of back-up:
	  ○ full
	  ○ incremental
	  ○ differential
	  ○ mirror.

1.24	**Understand the relationship between organisational policies and procedures and risk mitigation and be able to explain their importance in respect of adherence to security**
	• Organisational digital use policy:
	  ○ standard operating procedures for:
	  – network usage and control (for example monitoring bandwidth, identifying bottlenecks)
	  – internet usage (for example restricted access to sites, social media)
	  – bring your own device (BYOD)
	  – working from home (WFH) (for example DSE assessment)
	  – periodic renewal of password
	  – software usage (for example updating applications).
	• Health and safety policy for:
	  ○ standard operating procedures:
	  – lone working
	  – manual handling/safe lifting (for example moving hardware)
	  – working at height
	  – fire safety (for example staff training)
	  – Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013.
	• Change procedure – approval and documentation of all changes.
	• Auditing of policies and standard operating procedures – ensuring all actions are routinely examined (for example to ensure continued compliance).
	• Explain the purpose and application of each policy and procedure, summarising key information and using appropriate technical terms:
	  ○ digital use policy
	  ○ health and safety policy.
	• Explain the potential impact on security if policies and procedures are not adhered to (for example danger to life, privacy).
	(E5, D5)

1.25	**Understand the purpose and application of legislation, industry standards and regulatory compliance, and industry best practice guidelines for the security of information systems within digital infrastructure**
	• Legislation:
	  ○ EU General Data Protection Regulation (GDPR):
	  – purpose – standardises the way data is used, stored and transferred to protect privacy
	  – applications within digital infrastructure:
	  ▪ article 1 – subject matter and objectives
	  ▪ article 2 – material scope
	  ▪ article 3 – territorial scope
	  ▪ article 4 – definitions
	  ▪ article 5 – principles relating to processing of personal data

	▪ article 6 – lawfulness of processing ▪ article 7 – conditions for consent o Data Protection Act (DPA) 2018: – purpose – UK interpretation of GDPR to protect data and privacy – applications within digital infrastructure: ▪ used fairly, lawfully and transparently ▪ used for specified, explicit purposes ▪ used in a way that is adequate, relevant and limited to only what is necessary ▪ accurate and, where necessary, kept up-to-date ▪ kept for no longer than is necessary ▪ handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage o Computer Misuse Act 1990: – purpose – protects an individual's computer rights – applications within digital infrastructure: ▪ unauthorised access to computer materials (point 1 to 3) ▪ unauthorised access with intent to commit or facilitate commission of further offences (point 1 to 5) ▪ unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer (point 1 to 6). • Industry standards and regulatory compliance: o ISO 27001:2017: – purpose – certifiable standard for information security management – applications within digital infrastructure: ▪ GDPR/DPA 2018 ▪ information security ▪ information management ▪ penetration testing ▪ risk assessments o Payment Card Industry Data Security Standard (PCI DSS): – purpose – worldwide standard for protecting business card payments to reduce fraud – applications within digital infrastructure: ▪ build and maintain a secure network ▪ protect cardholder data ▪ maintain a vulnerability management program ▪ implement strong access control measures ▪ regularly monitor and test networks ▪ maintain an information security policy ▪ Industry best practice guidelines

	○ National Cyber Security Centre (NCSC) '10 Steps to Cyber Security': – purpose – inform organisations about key areas of security focus – applications within digital infrastructure: ▪ user education and awareness ▪ home and mobile working ▪ secure configuration ▪ removable media controls ▪ managing user privileges ▪ incident management ▪ monitoring ▪ malware protection ▪ network security ▪ risk management regime ○ Open Web Application Security Project (OWASP): – purpose: ▪ implement and review the usage of cyber security tools and resources ▪ implement education and training for the general public and for industry experts ▪ used as a networking platform – applications within digital infrastructure: ▪ support users with online security ▪ improve security of software solutions.
1.26	**Understand the principles of network security and their application to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data** • The CIA triad – confidentiality, integrity and availability applied to develop security. • Identification, authentication, authorisation and accountability (IAAA) – applied to prevent unauthorised access by implementing security policies to secure a network further: ○ applying directory services ○ security authentication process ○ using passwords and security implications ○ identification and protection of data ○ maintaining an up-to-date information asset register.
1.27	**Understand methods of managing and controlling access to digital systems and their application within the design of network security architecture** • Authentication – restricts or allows access based on system verification of user. • Firewalls – restricts or allows access to a defined set of services.

	• Intrusion detection system (IDS) – analyses and monitors network traffic for potential threats. • Intrusion prevention system (IPS) – prevents access based on identified potential threats. • Network access control (NAC) – restricts or allows access based on organisational policy enforcement on devices and users of network. • Mandatory access control (MAC) – restricts or allows access based on a hierarchy of security levels. • Discretionary access control (DAC) – restricts or allows access based on resource owner preference. • Attribute-based access control (ABAC) – restricts or allows access based on attributes or characteristics. • Role-based access control (RBAC) – restricts or allows access to resources based on the role of a user.

1.28	**Understand the physical and virtual methods of managing and securing network traffic and their application within the design of network security architecture**
	• Physical (for example server management, firewalls and cabling):
	  ○ software defined networking (SDN):
	  – transport layer security (TLS) (for example used in banking websites)
	  ○ demilitarised zone (DMZ)
	  ○ air gapping.
	• Virtual:
	  ○ virtual LAN (VLAN).
	• Subnets:
	  ○ virtual private network (VPN) (for example intranet, file systems, local network systems)
	  ○ virtual routing and forwarding (VRF)
	  ○ IP security (IPSec)
	  ○ air gapping.

1.29	**Understand the principles and applications of cyber security for internet connected devices, systems and networks**
	• The CIA (confidentiality, integrity and availability) triad – applied to assess the impact on security of systems (for example a data breach):
	  ○ protection and prevention against a cyberattack through secure configuration of a network
	  ○ limiting the network or system exposure to potential cyberattacks
	  ○ detection of cyberattacks and effective logging/auditing to identify impacts
	  ○ appropriate segregation of devices, networks and resources to reduce the impact of a cyberattack.

1.30	**Understand the techniques applied and be able to install and configure software to ensure cyber security for internet connected devices, systems and networks**
	• Security techniques:
	  ○ wireless security – WPA2 and WPA3 and use of end-to-end security implemented to monitor access to Wi-Fi systems
	  ○ device security – password/authentication implemented to improve device security
	  ○ encryption
	  ○ virtualisation
	  ○ penetration testing
	  ○ malware protection
	  ○ anti-virus protection
	  ○ software updates and patches
	  ○ multi-factor authentication
	  ○ single logout (SLO).
	• Install and configure software to secure the network:
	  ○ vulnerability scanning software (for example port scanning software, device scanning software)
	  ○ anti-malware software
	  ○ firewall software.
	• Apply device hardening to remove unnecessary software.
	• Check installation and configuration on end user devices.
	(E4, D1, D6)

1.31	**Understand the importance of cyber security to organisations and society**
	• Organisations:
	  ○ protection of:
	  – all systems and devices
	  – cloud services and their availability
	  – company data and information (for example commercially sensitive information)
	  – personnel data and data subjects (for example employee information, customer information)
	  ○ password protection policies for users and systems
	  ○ adherence to cyber security legislation to avoid financial, reputational and legal impacts
	  ○ protection against cybercrime.
	• Society:
	  ○ protection of personal information to:
	  – maintain privacy and security
	  – protect from prejudices
	  – ensure equal opportunities
	  – prevent identity theft.

	• Individuals' rights protected under DPA 2018:
	  ○ be informed about how data is being used
	  ○ access personal data
	  ○ have incorrect data updated
	  ○ have data erased
	  ○ stop or restrict the processing of data
	  ○ data portability (for example allowing individuals to access and reuse their data for different purposes)
	  ○ object to how data is processed in certain circumstances
	  ○ protection against cybercrime.

1.32	**Understand the fundamentals of network topologies and network referencing models and the application of cyber security principles**
	• Topologies:
	  ○ bus
	  ○ star
	  ○ ring
	  ○ token ring
	  ○ mesh
	  ○ hybrid
	  ○ client-server
	  ○ peer-to-peer.
	• Network referencing models:
	  ○ open systems interconnection (OSI) model:
	  – application layer
	  – presentation layer
	  – session layer
	  – transport layer
	  – network layer
	  – data link layer
	  – physical layer
	  ○ transmission control protocol/internet protocol (TCP/IP):
	  – application layer
	  – transport layer
	  – network layer
	  – network interface layer.
	• The minimum cyber security standards principles applied to network architecture:
	  ○ identify – management of risks to the security of the network, users and devices:
	  – assign cyber security lead
	  – risk assessments for systems to identify severity of different possible security risks
	  – documentation of configurations and responses to threats and vulnerabilities

	○ protect – development and application of appropriate control measures to minimise potential security risks: – implementation of anti-virus software and firewall – reduce attack surface – use trusted and supported operating systems and applications – decommission of vulnerable and legacy systems where applicable – performance of regular security audits and vulnerability checks – data encryption at rest and during transmission – assign minimum access to users – provide appropriate cyber security training ○ detect – implementation of procedures and resources to identify security issues: – installation and application of security measures – review audit and event logs – network activity monitoring ○ respond – reaction to security issues: – contain and minimise the impacts of a security issue ○ recover – restoration of affected systems and resources: – back-ups and maintenance plans to recover systems and data – continuous improvement review.
1.33	**Understand common vulnerabilities to networks, systems and devices and the application of cyber security controls** • Missing patches, firmware and security updates: ○ application of cyber security controls: – patch manager software – tracking network traffic – test groups/devices to test security. • Password vulnerabilities (for example missing, weak or default passwords, no password lockout allowing brute force or dictionary attacks): ○ application of cyber security controls: – minimum password requirements in line with up-to-date NCSC guidance (for example length, special character) – password reset policy. • Insecure basic input-output system (BIOS)/unified extensible firmware interface (UEFI) configuration: ○ application of cyber security controls: – review BIOS/UEFI settings – update BIOS. • Misconfiguration of permissions and privileges: ○ application of cyber security controls: – testing permissions and access rights to systems – scheduled auditing of permissions and privileges (for example remove access of terminated staff).

	• Unsecure systems due to lack of protection software:
	  ○ application of cyber security controls:
	  – protecting against malware (for example virus, worm, trojan, ransomware)
	  – update security software
	  – monitoring security software
	  – buffer overflow.
	• Insecure disposal of data and devices:
	  ○ application of cyber security controls:
	  – compliance with Waste Electrical and Electronic Equipment (WEEE) Directive 2013
	  – checking and wiping all data devices
	  ○ inadequate back-up management:
	  – application of cyber security controls:
	  ▪ back-up frequency
	  ▪ application of appropriate types of back-up.
	• Dynamic host configuration protocol (DHCP) spoofing:
	  ○ application of cyber security controls:
	  – using DHCP snooping.
	• VLAN attacks and VLAN hopping:
	  ○ application of cyber security controls:
	  – implementation testing of the VLAN
	  – scheduled testing and monitoring of network.
	• Misconfigured firewalls:
	  ○ application of cyber security controls:
	  – testing firewall
	  – scheduled monitoring and updates.
	• Exposed services and ports – allow network attacks (for example a user connecting their device to an ethernet port):
	  ○ application of cyber security controls:
	  – physical security controls
	  – monitoring network traffic.
	• Misconfigured access control lists (ACLs):
	  ○ application of cyber security controls:
	  – monitor and review ACLs.
	• Ineffective network topology design (for example inadequate placement of firewalls and DMZ):
	  ○ application of cyber security controls:
	  – review of network topology design prior to implementation
	  – implementation testing.
	• Unprotected physical devices:
	  ○ application of cyber security controls:
	  – install correct software.

Content area 2: Explain, install, configure, test and manage both physical and virtual infrastructure

What underpinning knowledge do students need?	

2.1	**Understand and be able to explain the principles of network and infrastructure design**
	• Resilience:
	  ○ high availability (HA) – primary and secondary configurations of systems to provide redundancy
	  ○ clustering – provides redundancy and scalability
	  ○ load balancing – directs network traffic based on load
	  ○ segmentation – network, systems, data, devices and services are split up to mitigate the potential impact of risks.
	• Quality of service (QoS) – used to guarantee a specific network service.
	• Number systems – applied for subnetting and IP addressing:
	  ○ binary
	  ○ hexadecimal
	  ○ decimal
	  ○ octal.
	• Explain the fundamentals of network infrastructure:
	  ○ identify and explain the purpose and application of network infrastructure
	  ○ summarise and explain, using correct technical language, the benefits of network infrastructure within an organisation
	  ○ identify and explain the application of protocols and ports.
	(E1, E4)

2.2	**Understand the principles of the transmission of digital information over copper cable, fibre cable and wireless networks and systems**
	• Signal type:
	  ○ electrical-based
	  ○ light-based
	  ○ wireless.
	• Security:
	  ○ tampering
	  ○ signal loss.
	• Segregation from electrical cables:
	  ○ susceptibility to interference:
	  – types of interference (for example electromagnetic impact on signal, static, crosstalk)
	  – mitigation techniques (for example shielding, run cables in parallel)
	  – adhering to industry standards:
	  ▪ BS EN 50174.

	• Wireless standards:
	  ○ 802.11b
	  ○ 802.11g
	  ○ 802.11n
	  ○ Wi-Fi 5
	  ○ Wi-Fi 6 and 6e
	  ○ Wi-Fi 7.
	• Internet protocol version 4 (IPv4) network and subnets:
	  ○ addressing schemes
	  ○ subnetting
	  ○ subnet masks.
	• Internet protocol version 6 (IPv6):
	  ○ IPv6 address types.

2.3	**Understand the elements of infrastructure and associated technologies**
	• Network devices:
	  ○ firewalls (for example next generation firewall (NGFW))/ unified threat management (UTM) appliances)
	  ○ routers
	  ○ switches
	  ○ hubs
	  ○ bridges
	  ○ wireless/Wi-Fi access points (APs).
	• Wireless range extenders:
	  ○ modems
	  ○ media converters.
	• End user devices (EUDs):
	  ○ desktops and laptops
	  ○ mobile devices (for example, smartphone, tablet)
	  ○ smart devices (for example, wearable technology, smart speakers)
	  ○ removable media (for example, external hard drive).
	• Storage devices and systems:
	  ○ hard disk drive (HDD)
	  ○ solid state drive (SSD)
	  ○ removable media (for example, USB flash drive, external hard drive)
	  ○ network-attached storage (NAS)
	  ○ storage area network (SAN)
	  ○ block storage
	  ○ object storage

	○ redundant array of independent disks (RAID): – RAID 0 – striping – RAID 1 – mirroring – RAID 5 – parity across drives – RAID 10 – mirroring and striping. • Wired and wireless technologies: ○ unshielded twisted pair (UTP) cable: – straight-through – crossover – EIA/TIA-568A layout – EIA/TIA-568B layout ○ RJ11 connectors ○ 8P8C/RJ45 connectors ○ copper cables (for example Cat 5e, Cat6) ○ fibre-optic cables ○ the point-to-point protocol (PPP) ○ SDN ○ Wi-Fi protected access (WPA) 1, 2, and 3. • Antennas: ○ omni-directional ○ directional ○ patch ○ yagi ○ dipole. • Cloud services: ○ IaaS ○ PaaS ○ SaaS ○ cloud storage. • Test equipment: ○ test plan ○ testing kit: – tone generator and probe – cable tester – tracing kit. • Support scripting (for example, automation and administration). • Network monitoring and logging. • Capacity management (for example, monitoring server load).
2.4	**Understand the requirements of static prevention and be able to assess risk when working with electrostatic sensitive equipment** • Mobility awareness (for example, limiting movement to avoid electrostatic discharge (ESD)). • Temperature/humidity checks (for example, increased humidity resulting in increased static electricity).

	• Application of static prevention equipment (for example, anti-static wrist strap).
	• Be able to assess workplace risk with regard to electrostatic discharge:
	  ○ apply the risk management process:
	  – identify:
	  ▪ possible risks
	  ▪ effect of actions on themselves and others
	  – calculate the probability and impact of the identified risk
	  – prioritise based on level of risk
	  – record and logically organise all relevant findings in the appropriate format
	  – apply appropriate ESD protection devices when working with hardware
	  – comply with all relevant health and safety standards and regulations
	  – record and store all documents in compliance with appropriate legislation and regulations.
	(E1, E3, M2, M6, M10, D5)

2.5	**Understand health and safety legislation and regulations in the workplace and their application in a digital infrastructure context** • Health and Safety at Work etc Act 1974 (for example, providing appropriate PPE, employer safeguarding). • Manual Handling Operations Regulations 1992 (for example, moving hardware). • Health and Safety (Display Screen Equipment) Regulations 1999 (as amended in 2002) (for example, reducing screen time, correctly configured workspaces). • Control of Substances Hazardous to Health (COSHH) Regulations 2002 (for example, printer maintenance). • Control of Major Accident Hazards (COMAH) Regulations 2015 (for example, earthing). • Waste Electrical and Electronic Equipment (WEEE) Directive 2013 (for example, removal or disposal of hardware or network components).

2.6	**Understand the advantages and limitations of physical servers:**
	• Advantages:
	  ○ full access to server resources required for business-critical operations
	  ○ fully customisable and configurable to business requirements.
	• Limitations:
	  ○ high purchase and running costs
	  ○ increased time allocation for maintenance
	  ○ storage cannot be scaled as easily as other server types
	  ○ requires physical space.

2.7	**Understand the advantages and limitations of self-hosted and cloud-hosted virtual servers**
	• Self-hosted server (virtual server on a physical host):
	  ○ advantages:
	  – lower expertise required to set up
	  – greater control of costs
	  – scaling can be applied
	  – high availability (HA)/clustering
	  ○ limitations:
	  – high upfront cost
	  – high cost for resilience.
	• Cloud-hosted virtual server (for example, Microsoft Azure, Amazon Web Services):
	  ○ advantages:
	  – scaling can be applied easily
	  – built in redundancy
	  – third-party support provided
	  ○ limitations:
	  – high subscription cost
	  – complex initial set-up.

2.8	**Understand the advantages and limitation of containers**
	• Advantages:
	  ○ require fewer system resources
	  ○ easily deployable owing to portability
	  ○ applications run more consistently and efficiently
	  ○ low operating and development costs.
	• Limitations:
	  ○ less secure if not configured correctly
	  ○ less flexibility on operating systems
	  ○ higher level of expertise required to set up and configure.

2.9	**Understand the types, benefits, similarities and differences of operating systems (OSs) and their application within digital infrastructure**
	• Types of operating systems:
	  ○ end user/desktop (for example Windows, macOS) – applied to desktop PCs and laptops
	  ○ mobile (for example Android, iOS) – applied to tablets and mobile devices
	  ○ server (for example Linux, Windows Server) – applied to client-server environments.
	• Benefits of operating systems:
	  ○ improved usability
	  ○ no required knowledge of machine language from user
	  ○ increased security of data.

	• Similarities across operating systems:
	  ○ provides user interface
	  ○ allows personalisation
	  ○ manages resources
	  ○ provides platform for installation of applications.
	• Differences between operating systems:
	  ○ specific features aligned to purpose (for example personal use, supporting client-server architecture)
	  ○ provides different levels of user experience (UX) and user interface (UI)
	  ○ supports varying types of functionality (for example touchscreen, wireless charging).

2.10	**Understand the service functions and their application within a client-server network environment** • Active directory domain services (AD DS): ○ active directory – provides functionality to centrally manage and organise user and device accounts, security groups and distribution lists, contained in organisational units (OUs). • Group policy – provides functionality to create group policy objects (GPOs) which can be applied to OUs. GPOs can be applied to deploy settings and files to users' profiles and devices, based on their OU. • Dynamic host configuration protocol (DHCP) – to assign IP addresses to network client devices. • Lightweight directory access protocol (LDAP) – used for directory services authentication. • Domain name system (DNS) – for the translation of hostnames to IP addresses. • File server and distributed file system (DFS) – to provide shared disk access. • Print server – to provide shared printer access. • Web, proxy and cache servers – to provide efficient internet/web access, security and filtering. • Mail servers – to handle the sending and receiving of emails to/from client mailboxes. • Application servers – to provide access to network-based applications. • Database servers – to provide backend shared databases. • Security utilities (for example, anti-virus) – to protect data or systems against loss or attack.

2.11	**Understand methods of remote access and how they protect data** • Virtual private network (VPN) – network is private and the connection is encrypted to prevent any unauthorised access. • Remote desktop protocol (RDP) (for example, proprietary RDP software) – data processing occurs on the machine being accessed, no data is transferred to the client machine. • Lights-out management (LOM) – the server can be remotely managed and many tasks carried out to address problems or unauthorised access. • Secure shell (SSH) – the connection is secure, only the 2 hosts can access the data.

2.12	**Understand the considerations involved in setting up a simple VPN to enable secure remote access**
	• Configuration of the VPN server:
	  ○ enabling the VPN service
	  ○ configuring IP address and DNS hostnames of the VPN interface
	  ○ managing user access, including authentication and permissions.
	• Configuration of the client device:
	  ○ creating the connection
	  ○ setting the destination IP address and fully qualified domain name (FQDN)
	  ○ setting permissions and conditions.

2.13	**Be able to install, configure and test physical and virtual networks**
	• Install and configure component parts of physical and virtual networks:
	  ○ server:
	  – types (for example physical, virtual)
	  – operating systems (for example Windows, Linux)
	  – applications:
	  – database (for example storage)
	  – security utilities (for example anti-virus)
	  ○ network infrastructure appropriate devices
	  ○ firewall
	  ○ load balancer
	  ○ end user devices (for example desktop PC, laptop, smartphone)
	  ○ network-based services (for example DNS, DHCP).
	• Select and apply appropriate network ports and protocols.
	• Implement appropriate scripting.
	• Apply appropriate back-up policies and procedures.
	• Implement testing to monitor quality of network:
	  ○ functionality
	  ○ performance
	  ○ record all test results to inform network improvements.
	(D1, D6)

2.14	**Be able to maintain the effective functioning of physical or virtual networks**
	• Maintain component parts of physical and virtual networks:
	  ○ server:
	  – types (for example, physical, virtual)
	  – operating systems
	  – applications:
	  – databases
	  – security utilities
	  ○ firewall
	  ○ load balancer
	  ○ network infrastructure devices
	  ○ network-based services:
	  – DNS
	  – DHCP.
	• Review and optimise performance:
	  ○ performance monitoring and logging systems (for example, email alerts)
	  ○ capacity management system (for example disk monitoring)
	  ○ software and hardware utilisation
	  ○ apply automation via scripting.
	(D1, D6)

2.15	**Be able to make and test an unshielded twisted pair (UTP) cable to required national and international standards**
	• Determine purpose of cable:
	  ○ calculate required length.
	• Make:
	  ○ straight-through cable
	  ○ crossover cable.
	• Select and apply appropriate equipment (for example, 8P8C/RJ45 connectors, crimper, wire cutters).
	• Test in compliance with applied TIA/EIA standards.
	(M2)

2.16	**Understand the principles of IT service management (ITSM)** • The co-creation of value through service relationships. • The delivery of great experience to customers. • Considering the broader scope and potential impact of changes. • Working across departments to learn how others use the systems.

2.17	**Understand the Information Technology Infrastructure Library (ITIL®) framework and how this is applied in a digital infrastructure context** • Service strategy – aligned to business objectives to ensure that the service is fit for purpose and fit for use. • Service design – design of services and all supporting elements for introduction into the live environment, ensuring that people, processes, products and partners are all considered. • Service transition – building and deploying services and ensuring that any changes are managed in a coordinated way. • Service operation – fulfilling requests, resolving failures, fixing problems and carrying out routine operational tasks. • Continual service improvement – continually improving the effectiveness and efficiency of IT processes and services.
2.18	**Understand the principles of disaster recovery plans (DRPs) and business continuity plans (BCPs)** • Key principles: o identify: – risk – operational critical systems – requirements (for example, resources) o analyse: – business impact (for example, impact on departments, customers, suppliers) – maximum downtime o design: – plan components o implement: – communication plan o measure: – test – compliance (for example, with relevant legislation, policies and procedures) – review and maintain.
2.19	**Understand the different purpose of BCPs and DRPs in the context of digital infrastructure** • BCP – planning and managing business continuity during a disruptive event: o alternative business premises o adaptive policies and processes o application of alternative technologies. • DRP – restoring normal business operations following a disaster (for example flood): o restoring functionality or access o replacement of infrastructure resources.

2.20	**Understand and be able to apply the stages within a solution lifecycle (SLC) in a digital infrastructure content**
	• Stages:
	  ○ discover:
	  – business requirements
	  – project definition and planning
	  – conceptual design
	  – feasibility and viability
	  ○ plan, design and develop:
	  – detailed design and planning
	  – proof of concept and prototyping
	  – compliance with organisational policies and standards
	  – utilisation of existing architecture and resources
	  – development
	  – integration
	  ○ testing and quality assurance:
	  – functional testing to ensure the product or service meets the agreed deliverables
	  – performance testing
	  ○ pre-production:
	  – sandboxed testing in a development environment
	  – sign-off and authorisation to deploy
	  ○ deployment:
	  – release into the live/production environment
	  – staged release plan for significant or high impact changes/updates
	  ○ monitor and evaluate ongoing performance:
	  – optimisation through continuous improvement in line with agreed change management processes
	  ○ decommission
	  ○ migrate to new solution.
	• Apply the stages of solution lifecycle in a safe and responsible manner:
	  ○ discover
	  ○ plan, design and develop
	  ○ test and quality assurance
	  ○ pre-production
	  ○ deployment
	  ○ monitor and evaluate ongoing performance
	  ○ decommission
	  ○ migrate to new solution.
	• Record and document decisions, actions and outcomes for each stage of the solution lifecycle.
	(M2, M3)

2.21	**Understand the principles, aims and benefits of a DevOps approach**
	• DevOps principles:
	  ○ continuous integration
	  ○ continuous delivery (for example, deployment)
	  ○ microservices
	  ○ infrastructure as code
	  ○ communication and collaboration
	  ○ automated testing
	  ○ adapt and scale
	  ○ monitoring and logging.
	• Aims:
	  ○ to deliver systems, applications or services in an agile way
	  ○ to build, test and release changes.
	• Benefits:
	  ○ rapid delivery of solutions (for example, through automation)
	  ○ increased productivity
	  ○ improved processes across teams
	  ○ scalability
	  ○ reduced errors.

2.22	**Understand the principles of solution architecture**
	• The importance of reuse.
	• The importance of documentation.
	• Solution architecture as applied to hardware.
	• Adherence to architecture frameworks (for example, The Open Group Architecture Framework (TOGAF)).
	• Alignment to enterprise architecture.
	• Architecture description:
	  ○ system
	  ○ view
	  ○ viewpoint
	  ○ concern
	  ○ stakeholder.

2.23	**Understand the concepts of virtualisation and the areas of application within digital infrastructure**
	• Concepts:
	  ○ the creation of many virtual resources from one physical resource (for example, partitioning)
	  ○ the creation of one virtual resource from one or more physical resources
	  ○ isolation
	  ○ encapsulation
	  ○ hardware independence.

	• Areas of application within digital infrastructure:
	  ○ network virtualisation
	  ○ server virtualisation
	  ○ desktop virtualisation
	  ○ operating system virtualisation
	  ○ data virtualisation.

2.24	**Be able to demonstrate continuous improvement by maintaining the effective functioning of a range of hardware solutions (for example contemporary, legacy) and network in response to change**
	• Identify and assess the change:
	  ○ identify the hardware affected by change
	  ○ assess the current performance of the network.
	• Apply the appropriate stages of a solution lifecycle to respond to change:
	  ○ assess the performance of the network after the response.
	• Process, analyse and review outcome data.
	• Record and logically organise all relevant findings and actions accurately and concisely using appropriate technical terms to inform future policies and procedures:
	  ○ summarise key information.
	(E1, E2, E4, D4)

Content area 3: Discover, evaluate and apply reliable sources of knowledge

What underpinning knowledge do students need?	

3.1	**Understand and be able to identify types of sources of knowledge that can be applied within digital infrastructure:**
	• Academic publications (for example, textbooks, research journals and periodicals).
	• Supplier literature (for example, handbooks or online articles for specific devices, computers or laptops).
	• Search engines (for example, Google, Bing).
	• Websites (for example, wikis, forums, Stack Overflow, manufacturers' websites).
	• Social media (for example, company profiles on Twitter/X, Facebook and LinkedIn).
	• Blogs (for example, reviews of new technologies, opinions on topical issues in the digital sector).
	• Vlogs (for example, demonstrations, tutorials on digital technologies).
	• Professional networks (for example, digital transformation networking events/conferences).
	• E-learning (for example, massive open online courses (MOOCs), recognised vendor qualifications, Cisco).
	• Peers (for example, colleagues, network contacts, other industry professionals).
	• Be able to identify sources of knowledge and apply factors that legitimise their use to meet requirements in a digital infrastructure context:
	  ○ identify and clarify the parameters of the requirements
	  ○ identify appropriate sources of knowledge (up to 3) (for example, search engines, blogs)
	  ○ apply the factors of reliability and validity to identified sources (for example, authority, date of publication)
	  ○ assess and review potential bias of sources
	  ○ assess and review the identified sources' appropriateness to meet the requirements.
	(E4, D1)

3.2	**Understand the factors of reliability and validity to be applied to legitimise the use of sources of knowledge:** • Industry-certified accreditation (for example, Cisco certified network associate (CCNA1), Microsoft technology associate (MTA), network fundamentals). • Appropriateness. • Evidence-based: ○ citations.

	• Relevant context.
	• Credibility of author:
	  ○ affiliated to specific bodies (for example, government, industry regulators)
	  ○ reputation
	  ○ experience (for example, relevant qualification in subject).
	• Target audience – produced with specific audience requirements taken into consideration (for example, use of technical/non-technical terminology).
	• Publication:
	  ○ version (for example, use of the current version)
	  ○ date of publication (for example, if the content is outdated).

3.3	**Be able to search for information to support a topic or scenarios within digital infrastructure and corroborate information across multiple sources** • Identify and clarify the parameters of the search (for example explore the future of the digital economy, identify trends in Big Data). • Identify the sources of data that contain the required information. • Safely and securely search sources for the information required. • Corroborate sources by applying cross-referencing across multiple sources. • Apply reliability and validity factors. • Assess and review potential bias of sources. (E4, D5)

3.4	**Understand the factors of bias and be able to identify bias when using sources of knowledge in a specific digital infrastructure context**
	• Types of conscious and unconscious bias:
	  ○ author/propriety bias – unweighted opinions of the author or owner
	  ○ confirmation bias – sources support a predetermined assumption
	  ○ selection bias – selection of sources that meets specific criteria
	  ○ cultural bias – implicit assumptions based on societal norms.
	• Indicators of bias within sources:
	  ○ partiality
	  ○ prejudice
	  ○ omission.
	• Bias reduction:
	  ○ based on fact/evidence
	  ○ inclusive approach.
	• Full representation of demographics:
	  ○ objectivity.

	• Identify bias: o identify the types of bias (for example confirmation, unconscious) o identify the indicators of bias within the source o explain clearly and concisely how bias has been created within the source o explain clearly and concisely how bias can be avoided within sources. (E1, E3, E5, M6, D3)
3.5	**Understand and be able to demonstrate the process of critical thinking and the application of evaluation techniques and tools** • Process of critical thinking: o identification of relevant information: – different arguments, views and opinions o analysis of identified information: – identify types of bias and objectivity – understand links between information and data o selection of relevant evaluation techniques and tools o evaluation of findings and drawing of conclusions o recording of conclusions. • Evaluation techniques: o formative evaluation o summative evaluation o qualitative (for example interviews, observations, workshops) o quantitative (for example experiments, surveys, statistical analysis) o benchmarking o corroboration: – cross-referencing – triangulation. • Evaluation tools: o gap analysis o KPI analysis o score cards o observation reports o user diaries o scenario mapping o self-assessment frameworks o maturity assessments. • Apply the process of critical thinking to meet requirements: o identify relevant information o analyse the information o select and apply appropriate evaluation techniques and tools

	○ evaluate findings ○ logically organise and record conclusions. • Select and apply techniques and tools to support evaluation in a digital infrastructure context: ○ identify and clarify the parameters of the evaluation ○ select appropriate techniques and tools to support the evaluation ○ apply the selected techniques and use the appropriate tools to support the evaluation ○ record the findings of the evaluation for the requirement. (E1, E3, E4, M5, M6, M8, D2, D3, D4)
3.6	**Understand methods of communication and sharing knowledge and their application within a digital infrastructure context** • Integrated and standalone IT service management tools: ○ incident and problem management systems ○ change management systems. • Knowledge bases and knowledge management systems. • Wikis and shared documents. • Shared digital workspaces. • Telephone. • Instant messaging. • Email. • Video conferencing. • Digital signage. • Social media: ○ organisational ○ public ○ personal. • Blogs. • Community forums. • Project management tools (for example, issue logs, Gantt charts, Kanban boards, burndown charts). • Policy, process and procedure documents.
3.7	**Be able to compare options of sources and rationalise the actions taken to ensure the reliability and validity of sources** • Identify the sources for comparison. • Apply the relevant reliability and validity factors to the sources. • Compare the outcomes of the validity and reliability actions. • Explain and recommend the choice of action to ensure the sources are reliable and valid, using appropriate technical terms. (E1, E3, E5, M5, D3)

2. Network Cabling

Content area 1: Apply procedures and controls to maintain the digital security of an organisation and its data

What underpinning knowledge do students need?	

1.1	**Understand the types of preventative business control techniques and be able to apply and maintain them in protecting the digital security of an organisation:**
	• Preventative control techniques:
	  ○ physical:
	  – specialist locks (anti-picking)
	  – barrier (for example fencing bollards)
	  – gates
	  – cages
	  – lock/key or equivalent
	  ○ combined – managed access:
	  – card readers
	  – biometric
	  – video
	  – pin/passcodes
	  ○ administrative, policies and procedures:
	  – separation of duties and relevance of role-based access.
	  ○ technical – domains and security policies:
	  – allowlist
	  – denylist
	  – access control lists
	  – sandboxing
	  – device hardening
	  – certificate authority.
	• Implement security controls in a business environment in line with NCSC cyber essentials:
	  ○ boundary firewalls
	  ○ secure configuration (for example enabling multi-factor authentication)
	  ○ access control
	  ○ malware protection
	  ○ patch management.
	• Configure and apply appropriate access control methods to physical or virtual networks (for example authentication, MAC, DAC, ABAC, RBAC).
	• Manage documents and data accurately in accordance with data protection legislation.
	(E5, D1, D6)

1.2	**Understand the types of detective business control techniques in protecting the digital security of an organisation**
	• Detective control techniques:
	  ○ physical:
	  – closed-circuit television (CCTV)
	  – motion sensors.
	  ○ administrative, policies and procedures:
	  – logs (for example, error logs)
	  – review/audit (for example, people entering and leaving the facilities).

1.3	**Understand the types of corrective business control techniques in protecting the digital security of an organisation**
	• Corrective control techniques:
	  ○ physical:
	  – fire suppression (for example, sprinklers, extinguishers)
	  – gas suppression systems (for example, inert and chemical gas systems).
	  ○ administrative, policies and procedures:
	  – standard operating procedure (for example, actions taken when a fire is identified).

1.4	**Understand the types of deterrent business control techniques in protecting the digital security of an organisation:**
	• Deterrent control techniques:
	  ○ physical:
	  – security guards
	  – alarm systems
	  – visible surveillance systems.
	  ○ administrative, policies and procedures:
	  – standard operating procedure (for example, setting alarm system, fire drill)
	  – employment contracts stipulating codes of conduct
	  – acceptable usage policies.

1.5	**Understand the types of directive business control techniques in protecting the digital security of an organisation**
	• Directive control techniques:
	  ○ physical:
	  – signage
	  – mandatory ID badge display (employees and visitors).
	  ○ administrative, policies and procedures:
	  – agreement types
	  – general security policies and procedures
	  – regular and compulsory staff training (for example, human firewall training).

1.6	**Understand the types of compensating business control techniques in protecting the digital security of an organisation**
	• Compensating control techniques:
	  ○ physical:
	  – temperature controls (for example, air conditioning).
	  ○ administrative, policies and procedures:
	  – role-based awareness training
	  – standard operating procedures (for example, environmental control monitoring).

1.7	**Be able to apply and monitor appropriate business control techniques and policies and procedures to ensure personal, physical and environmental security:**
	• Review the identified risk:
	  ○ gather information from system and users.
	• Select, apply and monitor appropriate business control techniques:
	  ○ preventative
	  ○ detective
	  ○ corrective
	  ○ deterrent
	  ○ directive
	  ○ compensating
	  ○ recovery.
	• Comply with relevant regulatory and organisational policies and procedures.
	(D3)

1.8	**Understand the components of a disaster recovery plan in protecting the digital security of an organisation:**
	• Disaster recovery plan (DRP):
	  ○ physical:
	  – back-ups
	  – off-site alternate storage.
	  ○ administrative, policies and procedures of a DRP supported by an organisational business continuity plan (BCP):
	  – ensuring all systems maintain functionality (for example arranging hardware)
	  – ensuring users can access systems away from the main building site
	  – deploying back-ups to maintain data integrity
	  – ensuring digital changes continue to meet business needs
	  – managing assets across the network and logging changes (for example, tagging and logging laptops)
	  – reporting infrastructure changes to management.

1.9	**Understand the types of impacts that can occur within an organisation as a result of threats and vulnerabilities** • Danger to life – breaches in health and safety policies (for example, injury and death). • Privacy – breaches of data (for example, compromised confidential business data, identity theft). • Property and resources – damage to property and systems. • Economic – financial loss or impairment. • Reputation – damage to brand and business value. • Legal – fines or prosecution.

1.10	**Understand potential vulnerabilities in critical systems**
	• Unauthorised access to network infrastructure.
	• Unauthorised physical access to network ports.
	• Single point of failure.
	• Open port access:
	  ○ universal serial bus (USB)
	  ○ network ports
	  ○ wireless networks.

1.11	Understand the impact of measures and procedures that are put in place to mitigate threats and vulnerabilities
	• Measures:
	  ○ recovery time objective (RTO)
	  ○ recovery point objective (RPO)
	  ○ mean time between failure (MTBF)
	  ○ mean time to repair (MTTR).
	• Procedures:
	  ○ standard operating procedure (SOP):
	  – installation procedure
	  – back-up procedure
	  – set-up procedure
	  ○ service level agreement (SLA):
	  – system availability and uptime
	  – response time and resolution timescales.

1.12	Understand the process of risk management
	• Process:
	  ○ identification – identifying potential risks, threats or vulnerabilities
	  ○ probability – likelihood of occurrence (for example, high, medium, low)
	  ○ impact – assess damage that can occur (for example, asset value)
	  ○ prioritisation – rank risks based on the analysis of probability and impact, ownership of risk
	  ○ mitigation – reducing probability or impact of risk.

1.13	**Understand approaches and tools for the analysis of threats and vulnerabilities**
	• Approaches:
	  ○ qualitative – non-numeric:
	  – determine severity using red, amber, green (RAG) rating:
	  – red – high risk requiring immediate action
	  – amber – moderate risk that needs to be observed closely
	  – green – low risk with no immediate action required
	  ○ quantitative – numeric:
	  – analyse effects of risk (for example, cost overrun, resource consumption).
	• Tools:
	  ○ fault tree analysis
	  ○ impact analysis
	  ○ failure mode effect critical analysis
	  ○ annualised loss expectancy (ALE)
	  ○ Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)
	  ○ strength, weakness, opportunity, threat (SWOT) analysis
	  ○ risk register – risk is identified and recorded using a RAG rating.

1.14	**Understand the factors involved in threat assessment for the mitigation of threats and vulnerabilities**
	• Environmental:
	  ○ extreme weather
	  ○ natural disaster
	  ○ animals (for example rodent chewing cables)
	  ○ humidity
	  ○ air quality.
	• Manmade:
	  ○ internal:
	  – malicious or inadvertent activity from employees and contractors
	  ○ external:
	  – malware
	  – hacking
	  – social engineering
	  – third-party organisations
	  – terrorism.
	• Technological:
	  ○ technology failures and faults (for example, Wi-Fi dropouts, inaccessible systems)
	  ○ device failure and faults (for example, firewall setting, interference of signal)
	  ○ impact of technical change (for example, system upgrade, software upgrade).

	• Political: ○ changes to legislation.

1.15	**Understand the purpose of and be able to carry out risk assessment in a network cabling context**
	• Purpose:
	  ○ to identify and reduce risk by:
	  – implementing Health and Safety Executive (HSE) guidelines to projects (for example, installing a new uninterruptible power supply (UPS) system into a server room and identifying risks to the installers)
	  – investigating risks within the project environment (for example, undertaking a PESTLE analysis)
	  – internal and external risk identification (for example, implementing a supply chain assessment)
	  – quantification of impact on asset value (for example financial loss as a result of downtime).
	• Conduct a security risk assessment in line with the risk management process for a system (for example a local area network cabling):
	  ○ assess the system and identify components
	  ○ apply the risk management process:
	  – identify possible risks within the system
	  – calculate the probability and impact of the identified risk
	  ○ analyse and prioritise based on level of risk to system
	  ○ record all relevant findings and actions accurately and concisely using appropriate technical terms.
	(E4, M6, D4)

1.16	**Understand the types of risk response within a network cabling context**
	• Types of response:
	  ○ accept – the impact of the risk is deemed acceptable (for example, low impact, low probability)
	  ○ avoid – change scope to avoid identified risk
	  ○ mitigate – reduce the impact or probability of the identified risk
	  ○ transfer – contractually outsource the risk to another party.

1.17	**Understand the process of penetration testing within network cabling**
	• Penetration testing (for example, wireless network tests):
	  ○ customer engagement
	  ○ information gathering
	  ○ discovery and scanning
	  ○ vulnerability testing
	  ○ exploitation
	  ○ final analysis and review
	  ○ utilise the test results.

1.18	**Understand the considerations in the design of a risk mitigation strategy** • Risk response (for example, accept, avoid, mitigate or transfer the risk). • User profile (for example, requirements, ability level). • Cost and benefit. • Assign an owner of the risk. • Escalation to appropriate authority within organisation. • Planning contingencies. • Monitoring and reviewing process.
1.19	Understand the purpose of technical security controls as risk mitigation techniques and their applications to business risks • Purpose – to improve network security for users and systems. • Technical security controls and their applications: o 5 cyber essentials controls: – boundary firewalls and internet gateways – restricting the flow of traffic in systems – secure configuration – ensuring user only has required functionality (for example, removing unnecessary software, configuration to limit web access) – malware protection – maintaining up-to-date anti-malware software and regular scanning – patch management – maintaining system and software updates to current levels – access control – restricting access to a minimum based on user attributes (for example principle of least privilege, username and password management). o device hardening – removing unneeded programs, accounts functions, applications, ports, permissions and access o remote monitoring and management (RMM) (for example, end user devices) o anti-virus software – protecting against attacks from established threats.
1.20	**Be able to demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a network cabling context** • Identify, gather and systematically organise information on incidents in Preparation for analysis. • Process and analyse trends in incident data to identify underlying risks. • Identify user profile (for example requirements, ability level). • Identify and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in end user devices (for example, placement of firewalls).

	• Monitor and review as part of a continuous improvement process:
	  ○ assign an owner of the risk
	  ○ plan contingencies.
	• Record all relevant findings and actions accurately and concisely using appropriate technical terms.
	(E4, M5, D4)

1.21	**Understand the purpose and types of encryption as a risk mitigation technique and their applications**
	• Purpose – to store and transfer data securely using cryptography.
	• Types of encryption and their applications:
	  ○ asymmetric encryption – applied to sending private data between 2 users (for example, encrypted email systems)
	  ○ symmetric encryption – applied to sending private data between 2 users using the same key (for example card payment systems)
	  ○ data at rest encryption:
	  – full disk encryption – applied to encrypt the contents of an entire hard drive using industry standard tool (for example, Windows, macOS)
	  – hardware security module (HSM) – safeguards digital keys to protect a device and its data from hacking
	  – trusted platform module (TPM) – applied to store encryption keys specific to the host device
	  ○ data in transit encryption:
	  – secure sockets layer (SSL) – applied to create an encrypted link between a website and a browser using security keys for businesses to protect the data on their websites
	  – transport layer security (TLS) – applied to encrypt end-to-end communication between networks (for example, in email, websites and instant messaging).

1.22	**Understand the purpose, criteria and types of back-up involved in risk mitigation**
	• Purpose:
	  ○ maintaining an up-to-date copy of data to enable future recovery and restoration (full disaster recovery or partial data loss).
	• Back-up criteria:
	  ○ frequency (for example periodic back-ups)
	  ○ source (for example files or data)
	  ○ destination (for example internal, external)
	  ○ storage (for example linear tape open (LTO), cloud, disk).
	• Types of back-up:
	  ○ full
	  ○ incremental
	  ○ differential
	  ○ mirror.

1.23	**Understand the relationship between organisation policies and procedures and risk mitigation and be able to explain their importance in respect of adherence to security**
	• Organisational digital use policy:
	  ○ standard operating procedures for:
	  – network usage and control (for example monitoring bandwidth, identifying bottlenecks)
	  – internet usage (for example restricted access to sites, social media)
	  – bring your own device (BYOD)
	  – working from home (WFH) (for example DSE assessment)
	  – periodic renewal of password
	  – software usage (for example updating applications).
	• Health and safety policy for:
	  ○ standard operating procedures:
	  – lone working
	  – manual handling/safe lifting (for example moving hardware)
	  – working at height
	  – fire safety (for example staff training)
	  – Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013.
	• Change procedure – approval and documentation of all changes.
	• Auditing of policies and standard operating procedures – ensuring all actions are routinely examined (for example to ensure continued compliance).
	• Explain the purpose and application of each policy and procedure, summarising key information and using appropriate technical terms:
	  ○ digital use policy
	  ○ health and safety policy.
	• Explain the potential impact on security if policies and procedures are not adhered to (for example, danger to life, privacy).
	(E5, D5)

1.24	**Understand the purpose and application of legislation, industry standards and regulatory compliance, and industry best practice guidelines for the security of information systems in a network cabling context**
	• Legislation:
	  ○ EU General Data Protection Regulation (GDPR):
	  – purpose – standardises the way data is used, stored and transferred to protect privacy
	  – applications within digital infrastructure:
	  ▪ article 1 – subject matter and objectives
	  ▪ article 2 – material scope
	  ▪ article 3 – territorial scope
	  ▪ article 4 – definitions
	  ▪ article 5 – principles relating to processing of personal data

	▪ article 6 – lawfulness of processing ▪ article 7–- conditions for consent o Data Protection Act (DPA) 2018: – purpose – UK interpretation of GDPR to protect data and privacy – applications within digital infrastructure: ▪ used fairly, lawfully and transparently ▪ used for specified, explicit purposes ▪ used in a way that is adequate, relevant and limited to only what is necessary ▪ accurate and, where necessary, kept up to date ▪ kept for no longer than is necessary ▪ handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage o Computer Misuse Act 1990: – purpose – protects an individual's computer rights – applications within digital infrastructure: ▪ unauthorised access to computer materials (point 1 to 3) ▪ unauthorised access with intent to commit or facilitate commission of further offences (point 1 to 5) ▪ unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer (point 1 to 6) • Industry standards and regulatory compliance: o ISO 27001:2017: – purpose – certifiable standard for information security management – applications within digital infrastructure: ▪ GDPR/DPA 2018 ▪ information security ▪ information management ▪ penetration testing ▪ risk assessments o Payment Card Industry Data Security Standard (PCI DSS): – purpose – worldwide standard for protecting business card payments to reduce fraud – applications within digital infrastructure: ▪ build and maintain a secure network ▪ protect cardholder data ▪ maintain a vulnerability management program ▪ implement strong access control measures ▪ regularly monitor and test networks ▪ maintain an information security policy.

	• Industry best practice guidelines:
	  ○ National Cyber Security Centre (NCSC) '10 Steps to Cyber Security':
	  – purpose – inform organisations about key areas of security focus
	  – applications within digital infrastructure:
	  ▪ user education and awareness
	  ▪ home and mobile working
	  ▪ secure configuration
	  ▪ removable media controls
	  ▪ managing user privileges
	  ▪ incident management
	  ▪ monitoring
	  ▪ malware protection
	  ▪ network security
	  ▪ risk management regime
	  ○ Open Web Application Security Project (OWASP):
	  – purpose:
	  ▪ implement and review the usage of cyber security tools and resources
	  ▪ implement education and training for the general public and for industry experts
	  ▪ used as a networking platform
	  – applications within digital infrastructure:
	  ▪ support users with online security
	  ▪ improve security of software solutions.

1.25	**Understand the principles of network security and their application to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data**
	• The CIA triad – confidentiality, integrity and availability applied to the development of security policies.
	• Identification, authentication, authorisation and accountability (IAAA) – applied to prevent unauthorised access by implementing security policies to secure a network further:
	  ○ applying directory services
	  ○ security authentication process
	  ○ using passwords and security implications
	  ○ identification and protection of data
	  ○ maintaining an up-to-date information asset register.

1.26	**Understand methods of managing and controlling access to digital systems and their application within the design of network security architecture** • Authentication – restricts or allows access based on system verification of user. • Firewalls – restricts or allows access to a defined set of services.

	• Intrusion Detection System (IDS) – analyses and monitors network traffic for potential threats. • Intrusion Prevention System (IPS) – prevents access based on identified potential threats. • Network Access Control (NAC) – restricts or allows access based on organisational policy enforcement on devices and users of network. • Mandatory Access Control (MAC) – restricts or allows access based on a hierarchy of security levels. • Discretionary Access Control (DAC) – restricts or allows access based on resource owner preference. • Attribute-Based Access Control (ABAC) – restricts or allows access based on attributes or characteristics. • Role-Based Access Control (RBAC) – restricts or allows access to resources based on the role of a user.

1.27	**Understand physical and virtual methods of managing and securing network traffic and their application within the design of network security architecture**
	• Physical (for example server management, firewalls and cabling):
	  ○ software defined networking (SDN):
	  – transport layer security (TLS) (for example used in banking websites)
	  ○ demilitarised zone (DMZ)
	  ○ air gapping.
	• Virtual:
	  ○ virtual LAN (VLAN):
	  – VPN (for example intranet, file systems, local network systems)
	  ○ virtual routing and forwarding (VRF)
	  ○ subnets
	  ○ IP security (IPSec)
	  ○ air gapping.

1.28	**Understand the principles and applications of cyber security for internet connected devices, systems and networks**
	• The confidentiality, integrity and availability (CIA) triad – applied to assess the impact on security of systems (for example, data breach):
	  ○ protection and prevention against a cyber-attack through secure configuration of a network
	  ○ limiting the network or system exposure to potential cyberattacks
	  ○ detection of cyber-attacks and effective logging/auditing to identify impacts
	  ○ appropriate segregation of devices, networks and resources to reduce the impact of a cyber-attack.

1.29	**Understand techniques applied to cyber security for internet connected devices, systems and networks** • Wireless security – WPA2 and WPA3 and end-to-end security implemented to monitor access to Wi-Fi systems. • Encryption. • Virtualisation. • Penetration testing. • Malware protection. • Software updates and patches. • Internet gateway security and access control. • Data leakage protection. • Multi-factor authentication. • Single logout (SLO).

1.30	**Understand the importance of cyber security to organisations and society**
	• Organisations:
	  ○ protection of:
	  – all systems and devices
	  – cloud services and their availability
	  – personnel data and data subjects (for example employee information, commercially sensitive information)
	  ○ password protection policies for users and systems
	  ○ adherence to cyber security legislation to avoid financial, reputational and legal impacts
	  ○ protection against cybercrime.
	• Society:
	  ○ protection of personal information to:
	  – maintain privacy and security
	  – protect from prejudices
	  – ensure equal opportunities
	  – prevent identity theft
	  ○ individuals' rights protected under DPA 2018:
	  – be informed about how data is being used
	  – access personal data
	  – have incorrect data updated
	  – have data erased
	  – stop or restrict the processing of data
	  – data portability (allowing individuals to get and reuse data for different services)
	  – object to how data is processed in certain circumstances
	  – protection against cybercrime.

1.31	Understand the fundamentals of network topologies and network referencing models and the application of cyber security principles
	• Topologies:
	  ○ bus
	  ○ star
	  ○ ring
	  ○ token ring
	  ○ mesh
	  ○ hybrid
	  ○ client-server
	  ○ peer-to-peer.
	• Network referencing models:
	  ○ Open Systems Interconnection (OSI) model:
	  – application layer
	  – presentation layer
	  – session layer
	  – transport layer
	  – network layer
	  – data link layer
	  – physical layer
	  ○ Transmission Control Protocol/Internet Protocol (TCP/IP):
	  – application layer
	  – transport layer
	  – network layer
	  – network interface layer.
	• The minimum cyber security standards principles applied to network architecture:
	  ○ identify – management of risks to the security of the network, users and devices:
	  – assign cyber security lead
	  – risk assessments for systems to identify severity of different possible security risks
	  – documentation of configurations and responses to threats and vulnerabilities
	  ○ protect – development and application of appropriate control measures to minimise potential security risks:
	  – implementation of anti-virus software and firewall
	  – reduce attack surface
	  – use trusted and supported operating systems and applications
	  – decommission of vulnerable and legacy systems where applicable
	  – performance of regular security audits and vulnerability checks
	  – data encryption at rest and during transmission
	  – assign minimum access to users
	  – provide appropriate cyber security training

	○ detect – implementation of procedures and resources to identify security issues: – installation and application of security measures – review audit and event logs – network activity monitoring ○ respond – reaction to security issues: – contain and minimise the impacts of a security issue ○ recover – restoration of affected systems and resources: – back-ups and maintenance plans to recover systems and data – continuous improvement review.
1.32	**Understand common vulnerabilities to networks, systems and devices and the application of cyber security controls** • Missing patches, firmware and security updates: ○ application of cyber security controls: – patch manager software – tracking network traffic – test groups/devices to test security. • Password vulnerabilities (for example, missing, weak or default passwords, no password lockout allowing brute force or dictionary attacks): ○ application of cyber security controls: – minimum password requirements in line with up-to-date NCSC guidance (for example, length, special character) – password reset policy. • Insecure basic input-output system (BIOS)/unified extensible firmware interface (UEFI) configuration: ○ application of cyber security controls: – review BIOS/UEFI settings – update BIOS. • Misconfiguration of permissions and privileges: ○ application of cyber security controls: – testing permissions and access rights to systems – scheduled auditing of permissions and privileges (for example, remove access of terminated staff). • Unsecure systems owing to lack of protection software: ○ application of cyber security controls: – protecting against malware (for example, virus, worm, trojan, ransomware) – update security software – monitoring security software – buffer overflow. • Insecure disposal of data and devices: ○ application of cyber security controls: – compliance with Waste Electrical and Electronic Equipment (WEEE) Directive 2013 – checking and wiping all data devices.

	• Inadequate back-up management:
	  ○ application of cyber security controls:
	  – back-up frequency
	  – application of appropriate types of back-ups.
	• unprotected physical devices:
	  ○ application of cyber security concepts
	  ○ install correct software.

Content area 2: Install and test cabling in line with technical and security requirements

What underpinning knowledge do students need?	

2.1	**Understand the principles of network cabling**
	• Representing data electronically:
	  ○ bits
	  ○ bytes
	  ○ packet structures.
	• Data transmission:
	  ○ synchronous transmission
	  ○ asynchronous transmission
	  ○ error detection
	  ○ error correction
	  ○ bandwidth limitation
	  ○ bandwidth noise
	  ○ data compression
	  ○ carrier-sense multiple access with collision detection (CSMA/CD)
	  ○ carrier-sense multiple access with collision avoidance (CSMA/CA).
	• Network interface cards.
	• Encapsulation:
	  ○ frames
	  ○ packets
	  ○ datagrams
	  ○ addresses
	  ○ sequence numbers.
	• Internet protocol version 4 (IPv4) network and subnets:
	  ○ addressing schemes
	  ○ subnetting
	  ○ subnet masks.
	• Internet protocol version 6 (IPv6):
	  ○ IPv6 address types.

2.2	**Understand tools and equipment used for network cabling and be able to demonstrate their effective use for a specific purpose in a network cabling context**
	• Network cabling tools:
	  ○ testing tools:
	  – multimeter
	  – tone generator and probe
	  – Optical Time Domain Reflectometer (OTDR)
	  – light source and power meter
	  – spectrum analyser
	  – continuity tester
	  ○ terminating tools:
	  – crimper
	  – copper cable stripper
	  – fibre optic stripper
	  – cable cutters
	  – punch-down tool (for example insulation displacement connector (IDC))
	  – screwdrivers
	  – fusion splicer
	  – fibre cleaning tools (for example alcohol wipes, punching cleaning tools, indirect viewing aids)
	  – cleave tool.
	• Physical access equipment:
	  ○ mobile elevating work platforms (MEWPs)
	  ○ low-level access towers
	  ○ step ladders.
	• Fixtures and fittings for telecommunications equipment:
	  ○ cabinets:
	  – prebuilt
	  – flat pack
	  ○ racks
	  ○ trunking/containment.
	• Apply network tools for a specific purpose:
	  ○ assess the parameters of the work being carried out
	  ○ select appropriate tool to meet parameters:
	  – testing tools (for example multimeter, tone generator and probe)
	  – terminating tools (for example crimper, copper cable stripper, fibre optic stripper)
	  ○ demonstrate safe application in compliance with manufacturers' guidelines of use.

2.3	**Understand networking devices used for network cabling**
	• Networking devices and components used in installing a network:
	  ○ firewalls
	  ○ routers
	  ○ switches:
	  – small form-factor plug (SFP)
	  ○ hubs
	  ○ bridges
	  ○ modems
	  ○ wireless access points (WAPs)
	  ○ media converter
	  ○ wireless range extender
	  ○ voice over IP (VoIP) endpoints
	  ○ CCTV
	  ○ servers
	  ○ network interfaces
	  ○ cabling.

2.4	**Be able to install and configure network devices on a network**
	• Interpret a network cabling design specification to identify appropriate location for installation.
	• Checking equipment meets the specification.
	• Confirm physical installation of network devices to meet a specific requirement (for example firewall, router, switch):
	  ○ assess physical space
	  ○ assess access to power
	  ○ assess cooling requirements.
	• Installation of devices into the appropriate cabinets/racks.
	• Test functionality of network devices.
	• Configure network devices to meet specific requirement.

2.5	**Understand the factors of structured network cabling design**
	• Architectural structure of network design:
	  ○ network topology:
	  – logical topologies
	  – physical topologies.
	• Physical design compliance with standards.
	• Relationship between permanent links and channels.
	• Context of campus distribution.
	• Relationship between passive network design and active network design.

2.6	**Understand the purpose and components of a network design specification and be able to design, analyse and interpret a specification**
	• Purpose:
	  ○ to provide the technical overview of the components.
	• Components:
	  ○ customer statement of requirement (SOR)
	  ○ bill of materials
	  ○ network cabling design documentation:
	  – building plans
	  – floorplans
	  – power and cooling diagram
	  – containment layout plans
	  – cabling routes plans
	  ○ installation administration:
	  – labelling
	  – documentation
	  – certification and warranty
	  – declaration of performance of cables
	  ○ installation procedures
	  ○ contractual penalties
	  ○ future-proofing/growth strategy.
	• Design, analyse and interpret a network cabling design specification:
	  ○ identify and gather user requirements of the network
	  ○ design a network cabling design specification:
	  – required components (for example, statement of requirements)
	  ○ analyse and interpret the network cabling design specification:
	  – identify quantity of resources needed (for example, people, hardware, software)
	  – calculate precise quantities of materials (for example, length of cable)
	  – assess location of components (for example, placement of cables, hardware, network devices)
	  ○ identify potential issues:
	  – equipment types
	  – quantity of resources and materials
	  – location
	  ○ the network cabling design specification must:
	  – use correct technical language and terms
	  – include appropriate plans, diagrams and design documentation to identify installation issues
	  – be organised logically and coherently.

2.7	**Understand the principles of light propagation in fibre cable**
	• Refraction.
	• Total internal reflection (TIR):
	  ○ transmission of light signal through the core of fibre cable:
	  – single mode
	  – multi-mode
	  ○ light signal is not absorbed by cladding of fibre cable enabling signal to travel long distances.

2.8	**Understand attenuation within the fibre channel**
	• Reduction in signal strength when the light signal is transmitted over a distance:
	  ○ measured in decibel (dB).
	• Considerations:
	  ○ analogue to digital conversion (for example where copper and fibre cable meet)
	  ○ electro-optical conversion
	  ○ synchronous transmission
	  ○ asynchronous transmission.
	• Causes of attenuation:
	  ○ absorption:
	  – absorption of light signal by particles in the fibre cable
	  – varies by material
	  – increases over longer distances
	  ○ scattering:
	  – light signal collides with particles inside the fibre cable
	  – light signal is absorbed into the cable cladding
	  ○ macrobends – large bends in the fibre cable
	  ○ microbends – small bends in the cable caused by mechanical stress
	  ○ asynchronous transmission.

2.9	**Understand causes of signal losses as a result of poor handling and installation techniques**
	• Dirty, faulty or contaminated connectors:
	  ○ unreliable connection
	  ○ no connection.
	• Excessive bending of cabling:
	  ○ under tension
	  ○ not under tension
	  ○ attenuation.
	• Poor quality fibre-optic cables and connectors:
	  ○ interference.

2.10	**Understand the principles of Ohm's law and its application to copper network cabling** • Ohm's law: o the relationship between voltage (V), current (I) and resistance (R): ▪ V = I x R – voltage (V) and current (I) are proportional: ▪ as voltage (V) increases, current (I) also increases – resistance (R) is the opposing force of current: ▪ as resistance (R) increases, current (I) decreases and slows down o application of Ohm's law to network cabling: o Ohm's law describes how a signal is transmitted from point A through a copper cable to point B for it to be received and translated to information o resistance: – varies with length of the cable – resistors present within the hardware – changes at different frequencies – different size cables for data transmission – maximum length cable to ensure efficient signal performance.
2.11	**Understand the features of copper and fibre media types and their applications** • Copper cable: o features: – durable – easy to handle – cheaper installation – high bandwidth – can provide power - Power over Ethernet (PoE) o applications: – telephony distribution – maximum limit of 90m (permanent links) – short run LAN within 100m total distance (channel links) o types: – twisted pair (TP): ▪ pairs of copper wires twisted together ▪ reduces electrical noise (due to twisting of the pairs) ▪ used for telephony-based circuits – unshielded twisted pair (UTP): ▪ no shielding ▪ reduces electrical noise (due to twisting of the pairs) ▪ reduces electromagnetic interference (EMI)

	– shielded/screened twisted pair (STP): ▪ reduces electrical noise (due to twisting of the pairs) ▪ shielded with insulating coating ▪ grounds wires ▪ protects from electromagnetic interference. – foil twisted pair (FTP): ▪ reduces electrical noise (due to twisting of the pairs) ▪ foil insulation coating. – coaxial: ▪ core copper wire ▪ plastic insulator around copper wire ▪ braided sheath to protect from electromagnetic interference ▪ outer coating to protect inner layers. • Fibre cable: ○ features: – greater transmission distance – higher bandwidth capabilities – greater channel carrying capacity – lightweight – less data degradation – cheaper material costs – limited by quality of laser at either end ○ applications: – large data transfer rates – interconnecting buildings – long distance connection points between different sites ○ types: – single mode: ▪ optical single mode 1 (OS1) ▪ optical single mode 2 (OS2) ▪ optical fibre core ▪ transmit single ray of light ▪ for use over longer distances – multi-mode: ▪ optical multi-mode 3 (OM3) ▪ optical multi-mode 4 (OM4) ▪ optical fibre core ▪ transmit multiple rays of light ▪ for use over shorter distances.

2.12	**Understand the advantages of using plenum fire resistant rated cable in network cabling installation over non-fire resistant cable** • Lower toxicity emission. • Lower smoke emission. • Reduced burning. • Reduced material breakdown. • Able to withstand higher levels of heat and remain fully operational. • Compliant with Construction Products Regulation (CPR).

2.13	**Understand types and features of connectors that can be applied within network cabling**
	• Connector types:
	  ○ copper:
	  – RJ-45
	  – RJ-11
	  – Bayonet Neill-Concelman (BNC)
	  – DB-9
	  – DB-25
	  – F-type
	  ○ fibre:
	  – local connector (LC)
	  – straight tip (ST)
	  – standard connector (SC)
	  – mechanical transfer registered jack (MT-RJ)
	  – multi-fibre push on (MPO).
	• Features of connector types:
	  ○ mating type (male-male, male-female, female-female)
	  ○ locking method/key and ease of connection:
	  – latching (for example, serial advanced technology attachment (SATA))
	  – screw down
	  – bayonet (for example, BNC)
	  – angled physical contact/ultra physical contact (APC/UPC)
	  ○ durability (for example, wear and general usage)
	  ○ variation in size
	  ○ insulation between pins (for example, strain relief boot).

2.14	**Understand the physical design of transceivers and the criteria for selection**
	• Physical design of transceivers:
	  ○ small form-factor pluggable (SFP)
	  ○ SFP+
	  ○ gigabit interface converter (GBIC)
	  ○ quad small form-factor pluggable (QSFP).
	• Criteria for selection of transceivers:
	  ○ simplex/duplex
	  ○ bidirectional
	  ○ bandwidth
	  ○ wave division multiplex
	  ○ dynamic range
	  ○ transfer rate
	  ○ connector type for transceivers
	  ○ housed in standalone unit or hosted in a network switch/router.

2.15	**Understand types of termination points and their applications**
	• 66 block:
	  ○ punch-down connection terminal for telephone systems
	  ○ terminate 22 to 26 solid copper wire
	  ○ RJ-21 female connector to receive male-end 25-pair cable
	  ○ for Cat3 copper cables
	  ○ used to connect cabling in a telephone system.
	• 110 block:
	  ○ supports higher speed networks than 66 block
	  ○ certified for:
	  – Cat5
	  – Cat6
	  – Cat6a
	  ○ used to terminate on-premises cabling in a structure cabling network
	  ○ supersedes 66 block.
	• Patch panel:
	  ○ contained within a mounted case
	  ○ incoming wires terminate in punch-down blocks
	  ○ patch cable used to interconnect cables by plugging in appropriate jacks
	  ○ handle large volume of copper and fibre cables
	  ○ used as wired network to accommodate ethernet cables.

2.16

Understand standards for copper and fibre cable, their methods of termination and ethernet deployment standards and be able to terminate cables in compliance with industry standards

- Copper cable standards:

Cable type	Cable rating frequency/ MHz	Cable length (max)/m	Ethernet data rate	Ethernet deployment standard
Cat3	16	100	10Mbps	10BASE-T
Cat5	100	100	100Mbps	100BASE-T / 100BASE-TX
Cat5e	100 (up to 350)	100	1Gbps	1000BASE-T
Cat6	250 (up to 550)	100	1Gbps/ 10Gbps	1000BASE-TX
Cat6a	500 (up to 550)	100	10Gbps	10GBASE-T
Cat7	600	100	10Gbps	-
RG59	High bandwidth	229	10Mbps	-
RG6	Low bandwidth	305	10Mbps	-

- Fibre cable standards:

Ethernet data rate	Wavelength/ nm	Cable length (max)/m				
		OS1/ OS2	OM1	OM2	OM3	OM4
100Mbps	850	40,000	2,000	2,000	2,000	2,000
1Gbps	850	100,000	275	550	550	1,000
10Gbps	850	40,000	33	82	300	550
40 & 100Gbps	850	40,000	-	-	100	150
1Gbps	1300	-	550	550	550	550
10Gbps	1300	-	300	300	300	300

- Termination methods:
  - patching – terminate copper or fibre cable to a patch panel
  - RJ45 – terminate copper cable for ethernet connection
  - splicing – connect fibre cable together:
    - fusion – connection between fibre cables is permanent:
      - used to connect single mode cables
    - mechanical – connection between fibre cables is not permanent:
      - used to connect single mode or multi-mode cables.

	• Termination standards:
	  ○ Telecommunications Industry Association (TIA)/ Electronic Industries Alliance (EIA) 568A:
	  – American standard
	  – pin-out colours adopted by TIA standards
	  ○ TIA/EIA 568B:
	  – British and European standard
	  – pin-out colours adopted by TIA standards
	  ○ crossover:
	  – used to connect 2 similar devices together (for example, one computer to another)
	  – one end of a crossover cable is terminated by TIA/EIA 568B, the other end is terminated by TIA/EIA 568A
	  – different colour code pin-out at each end of the cable
	  ○ straight-through:
	  – used to connect different devices to a network
	  – colour codes are the same at both ends of the cable (for example, TIA/EIA 568B on both ends)
	  ○ ethernet deployment standards:
	  – 100BaseT – uses 2 of the 4 pairs
	  – 100BaseTX – unidirectional 2 pairs Rx (receive) 2 pairs Tx (transmit)
	  – 1000BaseT – bidirectional 4 pair usage
	  – 1000BaseT1 – ethernet over single twisted pair (limited length)
	  – 1000BaseLX – (LX – long wavelength) single mode and multi-mode
	  – 1000BaseSX – (SX – short wavelength) multi-mode only
	  – 10GBaseT.
	• Apply patching to terminate copper and fibre cables:
	  ○ identify type of patching:
	  – copper
	  – fibre
	  ○ connect patch cables to allocated ports on the patch panel
	  ○ test patch cables to meet specification using appropriate testing tools
	  ○ review termination to ensure it conforms to industry standards:
	  – industry standards:
	  ▪ TIA/EIA 568A
	  ▪ TIA/EIA 568B
	  ▪ BS EN 61300.

2.17	**Understand maintenance processes of network to ensure efficient running of a network**
	• Troubleshooting network problems:
	  ○ identify a problem:
	  – fault occurs
	  – routine monitoring

	○ diagnostic: – information: ▪ investigate user actions ▪ network reporting tools – analysis of information: ▪ compare to previous data ▪ compare with similar system/device – consider possible causes: ▪ eliminate potential causes ▪ consider remaining possibilities ○ test remaining possibilities: – test the shortlist of possible causes – rule out possible causes that do not work – identify the correct cause ○ resolution: – implement the solution – document the cause and solution on a network plan (for example, hardware and software changes) – implement actions to mitigate against cause reoccurring. • Hardware and software installation/configuration: ○ resolution of identified security vulnerabilities: – apply fixes – maintaining compatibility of systems. ○ log all changes to hardware and software: – hardware updates – software updates ○ inform all necessary stakeholders/users of changes. • Monitoring and improving network performance: ○ network monitoring procedures: – monitor user activity – traffic and load – install network monitoring system (for example, packet analysers, firewalls) – track network performance benchmarks ○ predictive maintenance: – predicting life expectancy of network components and plan to replace ○ reactive maintenance: – reacting to component failure in a network – run to failure (RTF). • Retaining network components until natural failure or upgrade. • Continual service improvements.

2.18	**Understand common types of connectivity and performance failures that can occur in a network**
	• Network cabling connectivity and performance failures:
	  ○ physical:
	  – incorrect cable type (for example, unable to transmit signal)
	  – incorrect pin-out (for example, wire map errors)
	  – open/short (for example, missing connection or unintended connection)
	  – bad port (for example, dirty, faulty or contaminated connectors)
	  – damaged cables (for example, wiring faults, macrobending, microbending)
	  – bent pins
	  – duplex/speed mismatch (for example, incorrect cable)
	  – incorrect containment methods (for example, reduce signal strength, breach of standards and regulations)
	  ○ technical:
	  – attenuation
	  – latency
	  – jitter
	  – cross-talk
	  – electromagnetic interference (EMI)
	  – transceiver mismatch
	  – TX/RX reverse (for example, polarity mismatch/fibre mismatch)
	  – bottlenecks
	  – equipment hardware errors
	  – light emitting diode (LED) status indicators
	  ○ detection of performance failures:
	  – cyclical redundancy check
	  – encapsulation
	  – frame loss
	  – dropped packets
	  – dropped datagrams
	  – address conflicts
	  – missing sequence numbers
	  ○ analysis of performance benchmark.

2.19	**Understand the principles of transmission of digital information over copper and fibre cable**
	• Signal type:
	  ○ electrical-based
	  ○ light-based:
	  – laser
	  – LED.
	• Security:
	  ○ tampering
	  ○ signal loss.

	• Need for segregation from electrical cables:
	  ○ susceptibility to interference:
	  – types of interference (for example, electromagnetic impact on signal, static, crosstalk)
	  – mitigation techniques (for example, shielding, run cables in parallel)
	  – adhering to industry standards:
	  ▪ BS EN 50174.

2.20	**Understand the identification of media supporting other data services and the necessary precautions to prevent interference or damage to systems**
	• Identifying supporting media:
	  ○ telecommunications
	  ○ security systems (for example CCTV)
	  ○ alarm systems
	  ○ audio visual (AV) systems
	  ○ wireless access points (WAPs)
	  ○ Internet of Things (IoT) devices.
	• Precautions to mitigate interference or damage to systems:
	  ○ avoid common containment routes
	  ○ clearly label service cables
	  ○ refer to local authority installation records
	  ○ utilise effective change management
	  ○ plan and monitor integration of new supporting media:
	  – check records
	  – IP scanners
	  – check cable codes
	  – segregate wireless networks.

2.21	**Understand requirements and scope of compliance with legislation, regulations and standards**
	• Requirement of compliance with legislation, regulations and standards:
	  ○ legal obligations
	  ○ standardisation of work practices and processes (for example, production methods, materials used):
	  – risk management
	  ○ conforming to industry standards and requirements (for example, quality standard).
	• Scope of related standards:
	  ○ British Standards/European Norm (BS EN):
	  – BS EN 50173 (family of standards):
	  ▪ standards for generic cabling in different types of premises

	– BS EN 50174 (family of standards): ▪ standards for installation specification and quality assurance ▪ standards for installation planning and practices inside buildings ▪ standards for installation planning and practices outside buildings – BS EN 50310: ▪ application of equipotential bonding and earthing in buildings with information technology equipment – BS EN 60825: ▪ standards for safety of optical fibre communication systems (OFCS) o British Standards (BS): – BS 6701: ▪ specification for installation, operation and maintenance – BS 7671: ▪ Institute of Electrical and Electronics Engineers (IEEE) Wiring Regulations o IEEE: – IEEE 802.16: ▪ Worldwide Interoperability for Microwave Access (WiMAX) – IEEE 802.3 series: ▪ standard specification for ethernet. o International Electrotechnical Commission (IEC): – IEC60364: ▪ international standard on electrical installations for buildings. o Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA): – TIA/EIA-586-B: ▪ defines cable categories (Cat 3, Cat 5, Cat 5e, Cat 6) and their performance tests and procedures o International Organization for Standardization/International Electrotechnical Commission (ISO/IEC): – ISO/IEC11801: ▪ international standard for 'Generic Cabling for Customer Premises', dictates cable class o European Norm (EN): – EN50173: ▪ European standard for generic cabling, consistent with ISO/IEC11801 but includes additional requirements for network cabling o scope of related legislation and regulations: – Health and Safety at Work etc Act 1974: ▪ working with machine tools, working in confined spaces, personal protective equipment (PPE) – Electricity at Work Regulations 1989: ▪ working with electricity

	– Work at Height Regulations 2005: ▪ working at height – Control of Substances Hazardous to Health (COSHH) Regulations 2002: ▪ working with hazardous substances – Confined Spaces Regulation 1997: ▪ working in confined spaces – Personal Protective Equipment Regulation 2018: ▪ using appropriate personal protective equipment – Control of Asbestos Regulations 2012: ▪ asbestos-containing materials (ACM).
2.22	**Understand the process and management of the identification of asbestos-containing materials (ACM) identified during installation work and be able to explain the risk management if ACM are identified** • Actions required to reduce risk and impact of ACM: o application of risk management: – identify: ▪ stop work immediately ▪ informing relevant personnel (for example managers, peers) ▪ isolate and restrict access to the area – analysis of probability and impact: ▪ ensure area is investigated by an asbestos registered professional – prioritise and mitigate: ▪ outcomes based on investigation data ▪ removal or sealant of the material ▪ open air checks for contamination and fibres. • Risk management process: o undertake the risk management process to identify risk and record all outcomes: ▪ identification – request access to onsite register ▪ analysis of probability and impact ▪ prioritisation and mitigation ▪ record and logically organise all relevant findings and actions accurately and concisely using appropriate technical terms to inform future policies and procedures ▪ summarise key information.

2.23	**Be able to apply the risk management process to work safely at height using equipment to facilitate installation of network cabling**
	• Undertake the risk management process to identify risk and record all outcomes:
	  o identification
	  o probability
	  o impact
	  o prioritisation
	  o mitigation.
	• Demonstrate working at height in a safe manner using mobile elevating work platforms (MEWPs) in compliance with Health and Safety at Work etc Act 1974 regulations.
	• Assemble prefabricated low level access towers in compliance with manufacturers' guidelines.
	• Inspect prefabricated low level access towers in compliance with manufacturers' guidelines.
	• Operate prefabricated low level access towers in compliance with manufacturers' guidelines.
	• Dismantle prefabricated low level access towers in compliance with manufacturers' guidelines.

2.24	**Be able to apply the risk management process to ensure safe practices and procedures for working in confined spaces, in compliance with relevant health and safety legislation and regulations (for example, Health and Safety at Work etc Act 1974, Confined Spaces Regulations 1997)**
	• Undertake the risk management process to identify risk and record all outcomes:
	  o identification
	  o probability
	  o impact
	  o prioritisation
	  o mitigation.
	• Identify and apply appropriate PPE in compliance with legislation (for example, Health and Safety at Work etc Act 1974):
	  o maintaining PPE in compliance with manufacturers' guidelines.
	• Record and logically organise all relevant findings and actions accurately and concisely using appropriate technical terms to inform future policies and procedures:
	  o summarise key information.

2.25	**Be able to prepare, construct, arrange and install fixtures and fittings accurately to meet a specific network cabling requirement**
	• Interpret a network cabling design specification for the installation of fixtures and fittings for telecommunications equipment.
	• Compare the physical location against the specification:
	  ○ assess physical space
	  ○ assess access to power
	  ○ assess cooling requirements.
	• Construct and install appropriate cabinets/racks in compliance with manufacturers' guidelines and instructions:
	  ○ prebuilt or flat pack.
	• Install additional fixtures and fittings (for example trucking and containment).
	• Test all fixtures and fittings to ensure compliance with legislation, installation and safety requirements.
	• Arrange the equipment to meet the specification within the racks.

2.26	**Understand network cabling inspection parameters and standards**
	• Network cabling testing standards:
	  ○ TIA/EIA-568-B.2-1:
	  – the transmission performance specifications for 4-pair 100Ω Category 6 cabling.
	  ○ TIA/EIA-568-B.1-10:
	  – the transmission performance specifications for 4-pair 100Ω Augmented Category 6 Cabling Annex I
	  ○ TIA/EIA-TSB-155-A:
	  – guidelines for the assessment and mitigation of installed Category 6 cabling to support 10GBASE-T
	  ○ TIA-1152:
	  – requirements for field test instruments and measurements for balanced twisted pair cabling
	  ○ IEC 61935-1:
	  – specifies reference measurement procedures for cabling parameters.
	• Network cable certification process:
	  ○ test plan:
	  – scope
	  – approach
	  – resources
	  – schedule
	  ○ test equipment:
	  – copper test equipment (for examplecontinuity tester, networkcabling performance tester, cable certifier)
	  – fibre test equipment (for example optical loss test set (OLTS), visible light source, optical time domain reflectometer (OTDR), fibre inspection tool)

	○ test types and parameters: – copper cable tests (for example wiremap, cable length, near-end crosstalk (NEXT)) – fibre cable tests (for example tier 1 testing, tier 2 testing, fibre inspection) ○ test results analysis. • Consequences of failing to meet required standards: ○ network: – slower network speed – increased interference – difficult to maintain or upgrade – reduced cable lifetime – reduced security ○ business: – costs of revisit – service level agreement penalties – warranty penalties – reputational damage – delayed payments – failed external audits.
2.27	**Be able to carry out cable testing, applying appropriate testing tools, in accordance with equipment manufacturers' procedures and in compliance with TIA/EIA standards** • Identify the physical characteristics to be tested: ○ copper ○ fibre. • Identify the appropriate cable specification. • Apply appropriate testing methods to identified cable: ○ copper cabling testing and parameters (for example, wire map, cable length): – identify the appropriate testing tools – apply copper testing equipment in compliance with manufacturers' guidelines and industry standards (for example, continuity tester, network cabling performance tester, cable certifier) ○ fibre-optic cabling testing: – applying an optical loss test set (tier 1) in compliance with manufacturers' guidelines and industry standards – applying an optical time domain reflectometer (OTDR) (tier 2) in compliance with manufacturers' guidelines and industry standards – applying a fibre inspection tool in compliance with manufacturers' guidelines and industry standards. • Systematically record and organise test results.

2.28	**Be able to analyse and interpret copper and fibre test results** • Gather required data for analysis. • Use appropriate software to process test results. • Compare results against manufacturers' guidelines to ensure they are within accepted specification ranges. • Analyse and interpret test results. • Record and summarise reasoned conclusions based on the interpretation of data to meet intended purpose and user requirements.

2.29	**Understand the impact of poor quality workmanship and non-compliance with network cabling working practices**
	• Incorrect labelling of circuits, cables and equipment:
	  ○ increases the difficulty of:
	  – troubleshooting problems
	  – general maintenance
	  – adapting the network for different uses.
	• Failure to test all cabling:
	  ○ damage equipment
	  ○ premature breakdown
	  ○ impede services on the network
	  ○ non-identification of system errors.

Content area 3: Discover, evaluate and apply reliable sources of knowledge

What underpinning knowledge do students need?	

3.1	**Understand and be able to identify types of sources of knowledge that can be applied within network cabling**
	• Academic publications (for example, textbooks, research journals and periodicals).
	• Supplier literature (for example, handbooks or online articles for specific devices, computers or laptops).
	• Search engines (for example, Google, Bing).
	• Websites (for example, wikis, forums, Stack Overflow, manufacturers' websites).
	• Social media (for example company profiles for Twitter/X, Facebook and LinkedIn).
	• Blogs (for example, reviews of new technologies, opinions on topical issues in the digital sector).
	• Vlogs (for example, demonstrations, tutorials on digital technologies).
	• Professional networks (for example, digital transformation networking events/conferences).
	• E-learning (for example, massive open online courses (MOOCs), recognised vendor qualifications, Cisco).
	• Peers (for example, colleagues, network contacts, other industry professionals).
	• Be able to identify sources of knowledge and apply factors that legitimise their use to meet requirements in a network cabling context:
	  ○ identify and clarify the parameters of the requirements
	  ○ identify appropriate sources of knowledge (up to 3) (for example, search engines, blogs)
	  ○ apply the factors of reliability and validity to identified sources (for example, authority, date of publication)
	  ○ assess and review potential bias of sources
	  ○ assess and review the identified sources' appropriateness to meet the requirements.
	(E4, D1)

3.2	**Understand the factors of reliability and validity to be applied to legitimise the use of sources of knowledge** • Industry-certified accreditation (for example, Cisco certified network associate (CCNA1), Microsoft technology associate (MTA), network fundamentals). • Appropriateness. • Evidence-based: ○ citations.

	• Relevant context.
	• Credibility of author:
	  ○ affiliated to specific bodies (for example government, industry regulators)
	  ○ reputation
	  ○ experience (for example relevant qualification in subject)
	  – target audience – produced with specific audience requirements taken into consideration (for example use of technical/non-technical terminology).
	• Publication:
	  ○ version (for example use of the current version)
	  ○ date of publication (for example if the content is outdated).

3.3	**Be able to search for information to support a topic or scenarios within network cabling and corroborate information across multiple sources** • Identify and clarify the parameters of the search (for example explore the future of the digital economy, identify trends in Big Data). • Identify the sources of data that contain the required information. • Safely and securely search sources for the information required. • Corroborate sources by applying cross-referencing across multiple sources. • Apply reliability and validity factors. • Assess and review potential bias of sources. (E4, D5)

3.4	**Understand the factors of bias and be able to identify bias when using sources of knowledge in a specific network cabling context**
	• Bias – unweighted opinions of the author or owner
	  ○ confirmation types of conscious and unconscious bias:
	  – author/propriety bias – sources support a predetermined assumption
	  – selection bias – selection of sources that meets specific criteria
	  – cultural bias – implicit assumptions based on societal norms.
	• Indicators of bias within sources:
	  ○ partiality
	  ○ prejudice
	  ○ omission.
	• Bias reduction:
	  ○ based on fact/evidence
	  ○ inclusive approach:
	  – full representation of demographics.
	  ○ objectivity.

	• Identify bias:
	  o identify the types of bias (for example confirmation, unconscious)
	  o identify the indicators of bias within the source
	  o explain clearly and concisely how bias has been created within the source
	  o explain clearly and concisely how bias can be avoided within sources.

3.5	**Understand and be able to demonstrate the process of critical thinking and the application of evaluation techniques and tools**
	• Process of critical thinking:
	  o identification of relevant information:
	  – different arguments, views and opinions.
	• Analysis of identified information:
	  o identify types of bias and objectivity
	  o understand links between information and data
	  – selection of relevant evaluation techniques and tools
	  – evaluation of findings and drawing of conclusions
	  – recording of conclusions.
	• Evaluation techniques:
	  o formative evaluation
	  o summative evaluation
	  o qualitative (for example, interviews, observations, workshops)
	  o quantitative (for example, experiments, surveys, statistical analysis)
	  o benchmarking
	  o corroboration:
	  – cross-referencing
	  o triangulation.
	• Evaluation tools:
	  o gap analysis
	  o KPI analysis
	  o score cards
	  o observation reports
	  o user diaries
	  o scenario mapping
	  o self-assessment frameworks
	  o maturity assessments.
	• Apply the process of critical thinking to meet requirements:
	  o identify relevant information
	  o analyse the information
	  o select and apply appropriate evaluation techniques and tools
	  o evaluate findings
	  o logically organise and record conclusions.

	• Select and apply techniques and tools to support evaluation in a network cabling context:
	  ○ identify and clarify the parameters of the evaluation
	  ○ select appropriate techniques and tools to support the evaluation
	  ○ apply the selected techniques and use the appropriate tools to support the evaluation
	  ○ record the findings of the evaluation for the requirement.
	(E1, E3, E4, M5, M6, M8, D2, D3, D4)

3.6	**Understand methods of communication and sharing knowledge and their application within a network cabling context**
	• Integrated and standalone IT service management tools:
	  ○ incident and problem management systems
	  ○ change management systems.
	• Knowledge bases and knowledge management systems.
	• Wikis and shared documents.
	• Shared digital workspaces.
	• Telephone.
	• Instant messaging.
	• Email.
	• Video conferencing.
	• Digital signage.
	• Social media:
	  ○ organisational
	  ○ public
	  ○ personal.
	• Blogs.
	• Community forums.
	• Project management tools (for example issue logs, Gantt charts, Kanban boards, burndown charts).
	• Policy, process and procedure documents.

3.7	**Be able to compare options of sources and rationalise the actions taken to ensure the reliability and validity of sources** • Identify the sources for comparison. • Apply the relevant reliability and validity factors to the sources. • Compare the outcomes of the validity and reliability actions. • Explain and recommend the choice of action to ensure the sources are reliable and valid, using appropriate technical terms. (E1, E3, E5, M5, D3)

Content area 1: Apply procedures and controls to maintain the digital security of an organisation and its data

What underpinning knowledge do students need?	

1.1	**Understand the types of preventative business control techniques and be able to apply and maintain them in protecting the digital security of an organisation**
	• Preventative control techniques:
	  ○ physical:
	  – specialist locks (anti-picking)
	  – barriers (for example, fencing, bollards)
	  – gates
	  – cages
	  – flood defence systems
	  – temperature control (for example, air conditioning)
	  ○ combined – managed access:
	  – card readers
	  – biometric
	  – video
	  – pin/passcodes
	  ○ administrative, policies and procedures:
	  – separation of duties and relevance of role-based access
	  ○ technical – domains and security policies:
	  – allowlist
	  – denylist
	  – access control lists
	  – sandboxing
	  – device hardening
	  – certificate authority.
	• Set up a domain services environment with security controls (for example, group-based security and permissions, password complexity).
	• Set up and deploy a certificate authority (for example, directory certificate services – install onto PC).
	• Implement security controls in a business environment in line with NCSC cyber essentials:
	  ○ boundary firewalls
	  ○ secure configuration (for example, enabling multi-factor authentication (MFA))
	  ○ access control
	  ○ malware protection
	  ○ patch management.

	• Configure and apply appropriate access control methods to end user devices (for example, authentication, MAC, DAC, ABAC, RBAC). • Manage documents and data accurately in accordance with data protection legislation. (E5, D1, D5, D6)
1.2	**Understand the types of detective business control techniques in protecting the digital security of an organisation** • Detective control techniques: ○ physical: – closed-circuit television (CCTV) – motion sensors ○ administrative, policies and procedures: – logs (for example, logs of temperature in server room, error logs) – review/audit (for example, people entering and leaving the facilities).
1.3	**Understand the types of corrective business control techniques in protecting the digital security of an organisation** • Corrective control techniques: ○ physical: – fire suppression (for example, sprinklers, extinguishers) – gas suppression (for example, inert and chemical gas systems) ○ administrative, policies and procedures: – standard operating procedure (for example, actions taken when a fire is identified).
1.4	**Understand the types of deterrent business control techniques in protecting the digital security of an organisation** • Deterrent control techniques: ○ physical: – security guards – alarm systems – visible surveillance systems ○ administrative, policies and procedures: – standard operating procedure (for example, setting alarm system, fire drill) – employment contracts stipulating codes of conduct – acceptable usage policies.

1.5	**Understand the types of directive business control techniques in protecting the digital security of an organisation**
	• Directive control techniques:
	  ○ physical:
	  – signage
	  – mandatory ID badge display (employees and visitors)
	  ○ administrative, policies and procedures:
	  – agreement types
	  – general security policies and procedures
	  – regular and compulsory staff training (for example, human firewall training).

1.6	**Understand the types of compensating business control techniques in protecting the digital security of an organisation**
	• Compensating control techniques:
	  ○ physical:
	  – temperature controls (for example, air conditioning)
	  ○ administrative, policies and procedures:
	  – role-based awareness training
	  – standard operating procedures (for example, environmental control monitoring).

1.7	**Be able to apply and monitor appropriate business control techniques and policies and procedures to ensure personal, physical and environmental security**
	• Review the identified risk:
	  ○ gather information from system and users.
	• Select, apply and monitor appropriate business control techniques:
	  ○ preventative
	  ○ detective
	  ○ corrective
	  ○ deterrent
	  ○ directive
	  ○ compensating
	  ○ recovery.
	• Comply with relevant regulatory and organisational policies and procedures.
	(D3)

1.8	**Understand components of a disaster recovery plan in protecting the digital security of an organisation**
	• Disaster recovery plan (DRP) components:
	  ○ physical:
	  – back-ups
	  – off-site alternative storage of servers

	○ administrative, policies and procedures of a DRP supported by an organisational business continuity plan (BCP): – ensuring all systems maintain functionality (for example, arranging hardware) – ensuring users can access systems away from the main building site – deploying back-ups to maintain data integrity – ensuring digital changes continue to meet business needs – managing assets across the network and logging changes (for example, tagging and logging laptops) – reporting infrastructure changes to management.
1.9	**Understand the types of impacts that can occur within an organisation as a result of threats and vulnerabilities** • Danger to life – breaches in health and safety policies (for example, injury and death). • Privacy – breaches of data (for example, compromised confidential business data, identity theft). • Property and resources – damage to property and systems. • Economic – financial loss or impairment. • Reputation – damage to brand and business value. • Legal – fines, prosecution.
1.10	**Understand the potential vulnerabilities in critical systems** • Unauthorised physical access to network ports. • User account control. • Single point of failure. • Open port access: ○ universal serial bus (USB) ○ network ports. • Wireless networks.
1.11	**Understand the impact of measures and procedures that are put in place to mitigate threats and vulnerabilities** • Measures: ○ recovery time objective (RTO) ○ recovery point objective (RPO) ○ mean time between failure (MTBF) ○ mean time to repair (MTTR). • Procedures: ○ standard operating procedure (SOP): – installation procedure – back-up procedure – set-up procedure. ○ service level agreement (SLA): – system availability and uptime – response time and resolution timescales.

1.12	**Understand the process of risk management**
	• Process:
	  ○ identification – identifying potential risk or threats and vulnerabilities
	  ○ probability – likelihood of occurrence (for example, high, medium, low)
	  ○ impact – assess damage that can occur (for example, asset value)
	  ○ prioritisation – rank risks based on the analysis of probability and impact, ownership of risk
	  ○ mitigation – reducing probability or impact of risk.

1.13	**Understand approaches and tools for the analysis of threats and vulnerabilities**
	• Approaches:
	  ○ qualitative – non-numeric:
	  – determine severity using red, amber, green (RAG) rating:
	  ▪ red – high risk requiring immediate action
	  ▪ amber – moderate risk that needs to be observed closely
	  ▪ green – low risk with no immediate action required
	  ○ quantitative – numeric:
	  – analyse effects of risk (for example cost overrun, resource consumption).
	• Tools:
	  ○ fault tree analysis
	  ○ impact analysis
	  ○ failure mode effect critical analysis
	  ○ annualised loss expectancy (ALE)
	  ○ Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)
	  ○ strength, weakness, opportunity, threat (SWOT) analysis
	  ○ risk register – risk is identified and recorded using a RAG rating.

1.14	**Understand factors involved in threat assessment for the mitigation of threats and vulnerabilities**
	• Environmental:
	  ○ extreme weather
	  ○ natural disaster
	  ○ animals (for example, rodent in server room)
	  ○ humidity
	  ○ air quality.
	• Manmade:
	  ○ internal:
	  – malicious or inadvertent activity from employees and contractors

	○ external: – malware – hacking – social engineering – third-party organisations – terrorism. • Technological: ○ technology failures and faults: – misconfigured devices – Wi-Fi dropouts – inaccessible systems – VPN not connecting – expired passwords ○ device failure and faults (for example, laptops, tablets, telephones): – hard disk failure – RAM failure – damaged peripherals ○ system failures and faults: – software breakages/corruption – inaccessible websites ○ impact of technical change: – potential downtime – system/software upgrades – misconfigured systems. • Political: ○ changes/amendments in legislation.
1.15	**Understand the purpose of and be able to carry out risk assessment in a digital support context** • Purpose: ○ to identify and reduce risk by: – implementing Health and Safety Executive (HSE) guidelines to projects (for example, supporting users with safe ergonomic equipment usage and accessibility) – investigating risks within the project environment (for example, undertaking a PESTLE analysis) – internal and external risk identification (for example, system access for employees and contractors) – quantification of impact on asset value (for example, financial loss as a result of downtime). • Conduct a security risk assessment in line with the risk management process for a system (for example, BYOD): ○ assess the system and identify components. • Apply the risk management process: ○ identify possible risks within the system ○ calculate the probability and impact of the identified risk

	○ analyse and prioritise based on level of risk to system ○ record all relevant findings and actions accurately and concisely using appropriate technical terms. (E4, M6, D4)
1.16	**Understand types of risk response within a digital support context** • Types of response: ○ accept – the impact of the risk is deemed acceptable ○ avoid – change scope to avoid identified risk ○ mitigate – reduce the impact or probability of the identified risk ○ transfer – contractually outsource the risk to another party.
1.17	**Understand the process of penetration testing within digital suppo**rt • Penetration testing (for example wireless network tests): ○ customer engagement ○ information gathering ○ discovery and scanning ○ vulnerability testing ○ exploitation ○ final analysis and review ○ utilise the test results.
1.18	**Understand the considerations in the design of a risk mitigation strategy and be able to demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a digital support context** • Risk response (for example, accept, avoid, mitigate or transfer the risk). • User profile (for example, requirements, ability level). • Cost and benefit. • Escalation to appropriate authority within organisation. • Identify, gather and systematically organise information on incidents in preparation for analysis. • Process and analyse trends in incident data to identify underlying risks. • Identify user profile (for example, requirements, ability level). • Identify and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in end user devices (for example, installing RMM software, device hardening). • Monitor and review as part of a continuous improvement process: ○ assign an owner of the risk ○ plan contingencies ○ update devices with current security software ○ interpret the outputs of penetration testing.

1.19	**Understand the purpose of technical security controls as risk mitigation techniques and their applications to business risks within a digital support context**
	• Purpose – to improve network security for users and systems.
	• Technical security controls and their applications:
	  o 5 cyber essentials controls:
	  – access control – restricting access to a minimum based on user attributes (for example, principle of least privilege, username and password management)
	  – patch management – maintaining system and software updates to current levels
	  – malware protection – maintaining up-to-date anti-malware/ anti-virus software and regular scanning
	  – boundary firewalls and internet gateways – restricting the flow of traffic in systems
	  – secure configuration – ensuring user only has required functionality (for example, removing unnecessary software, configuration to limit web access)
	  o device hardening – removing unneeded programs, accounts functions, applications, ports, permissions and access
	  o remote monitoring and management (RMM) (for example, end user devices)
	  o vulnerability scanning (for example, port scanning, device scanning).

1.20	**Be able to demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a digital support context**
	• Identify, gather and systematically organise information on incidents in Preparation for analysis.
	• Process and analyse trends in incident data to identify underlying risks.
	• Identify user profile (for example, requirements, ability level).
	• Identify and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in end user devices (for example, installing RMM software, device hardening).
	• Monitor and review as part of a continuous improvement process:
	  o assign an owner of the risk
	  o plan contingencies
	  o update devices with current security software
	  o interpret the outputs of penetration testing
	  o record all relevant findings and actions accurately and concisely using appropriate technical terms.
	(E4, M5, D4)

1.21	**Understand the purpose and types of encryption as a risk mitigation technique and their applications**
	• Purpose – to store and transfer data securely using cryptography.
	• Types of encryption and their applications:
	  ○ asymmetric encryption – applied to send private data from one user to another (for example, encrypted email systems)
	  ○ symmetric encryption – applied to encrypt and decrypt a message using the same key (for example, card payment systems).
	• Data at rest encryption:
	  ○ full disk encryption – applied to encrypt the contents of an entire hard drive using industry standard tool (for example, Windows, macOS)
	  ○ HSM – safeguards digital keys to protect a device and its data from hacking
	  ○ TPM – applied to store encryption keys specific to the host device.
	• Data in transit encryption:
	  ○ SSL – applied to create an encrypted link between a website and a browser using security keys for businesses to protect the data on their websites
	  ○ TLS – applied to encrypt end-to-end communication between networks (for example, in email, websites and instant messaging).

1.22	**Understand the purpose, criteria and types of back-up involved in risk mitigation**
	• Purpose:
	  ○ maintaining an up-to-date copy of data to enable future recovery and restoration (for example, full disaster recovery or partial data loss).
	• Back-up criteria:
	  ○ frequency (for example, periodic back-ups)
	  ○ source (for example, files or data)
	  ○ destination (for example, internal, external)
	  ○ storage (for example, linear tape open (LTO), cloud, disk).
	• Types of back-up:
	  ○ full
	  ○ incremental
	  ○ differential
	  ○ mirror.

1.23	**Understand the relationship between organisational policies and procedures and risk mitigation and be able to explain their importance in respect of adherence to security**
	• Organisational digital use policy:
	  ○ standard operating procedures for:
	  – network usage and control (for example, monitoring bandwidth, identifying bottlenecks)
	  – internet usage (for example, restricted access to sites, social media)
	  – bring your own device (BYOD)
	  – working from home (WFH) (for example, DSE assessment)
	  – periodic renewal of password
	  – software usage (for example, updating applications).
	• Health and safety policy for:
	  ○ standard operating procedures:
	  – lone working
	  – manual handling/safe lifting (for example, moving hardware)
	  – working at height
	  – fire safety (for example, staff training)
	  – Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013.
	• Change procedure – approval and documentation of all changes:
	  ○ auditing of policies and standard operating procedures – ensuring all actions are routinely examined (for example, to ensure continued compliance).
	• Explain the purpose and application of each policy and procedure, summarising key information and using appropriate technical terms:
	  ○ digital use policy
	  ○ health and safety policy.
	• Explain the potential impact on security if policies and procedures are not adhered to (for example, danger to life, privacy).
	(E5, D5)

1.24	**Understand the purpose and application of legislation, industry standards and regulatory compliance, and industry best practice guidelines for the security of information systems in the context of digital support**
	• Legislation:
	  ○ EU General Data Protection Regulation (GDPR):
	  – purpose – standardises the way data is used, stored and transferred to protect privacy
	  – applications within digital support:
	  ▪ article 1 – subject matter and objectives
	  ▪ article 2 – material scope
	  ▪ article 3 – territorial scope
	  ▪ article 4 – definitions
	  ▪ article 5 – principles relating to processing of personal data

	▪ article 6 – lawfulness of processing ▪ article 7 – conditions for consent. o Data Protection Act (DPA) 2018: – purpose – UK interpretation of GDPR to protect data and privacy – applications within digital support: ▪ used fairly, lawfully and transparently ▪ used for specified, explicit purposes ▪ used in a way that is adequate, relevant and limited to only what is necessary ▪ accurate and, where necessary, kept up-to-date ▪ kept for no longer than is necessary ▪ handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage o Computer Misuse Act 1990: – purpose – protects an individual's computer rights – applications within digital support: ▪ unauthorised access to computer materials (point 1 to 3) ▪ unauthorised access with intent to commit or facilitate commission of further offences (point 1 to 5) ▪ unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer (point 1 to 6). • Industry standards and regulatory compliance: o ISO 27001:2017: – purpose – certifiable standard for information security management – applications within digital support: ▪ GDPR/DPA 2018 ▪ information security ▪ information management ▪ penetration testing ▪ risk assessments. o Payment Card Industry Data Security Standard (PCI DSS): – purpose – worldwide standard for protecting business card payments to reduce fraud – applications within digital support: ▪ build and maintain a secure network ▪ protect cardholder data ▪ maintain a vulnerability management program ▪ implement strong access control measures ▪ regularly monitor and test networks ▪ maintain an information security policy.

	• Industry best practice guidelines:
	  ○ National Cyber Security Centre (NCSC) '10 Steps to Cyber Security':
	  – purpose – inform organisations about key areas of security focus
	  – applications within digital support:
	  ▪ user education and awareness
	  ▪ home and mobile working
	  ▪ secure configuration
	  ▪ removable media controls
	  ▪ managing user privileges
	  ▪ incident management
	  ▪ monitoring
	  ▪ malware protection
	  ▪ network security
	  ▪ risk management regime.
	  ○ Open Web Application Security Project (OWASP):
	  – purpose:
	  ▪ implements and reviews the usage of cyber security tools and resources
	  ▪ implements education and training for the general public and for industry experts
	  ▪ used as a networking platform.
	  – applications within digital support:
	  ▪ support users with online security
	  ▪ improve security of software solutions.

1.25	**Understand the principles of network security and their application to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data**
	• The CIA triad – confidentiality, integrity and availability applied to the development of security policies.
	• IAAA (identification, authentication, authorisation and accountability) – applied to prevent unauthorised access by implementing security policies to secure a network further:
	  ○ applying directory services
	  ○ security authentication process
	  ○ using passwords and security implications
	  ○ identification and protection of data
	  ○ maintaining an up-to-date information asset register.

1.26	**Understand methods of managing and controlling access to digital systems and their application within the design of network security architecture** • Authentication – restricts or allows access based on system verification of user. • Firewalls – restricts or allows access to a defined set of services.

	• Apply and monitor appropriate access control methods to support physical and virtual infrastructure as required:
	  ○ intrusion detection system (IDS) – analyses and monitors network traffic for potential threats
	  ○ intrusion prevention system (IPS) – prevents access based on identified potential threats
	  ○ network access control (NAC) – restricts or allows access based on organisational policy enforcement on devices and users of network
	  ○ mandatory access control (MAC) – restricts or allows access based on a hierarchy of security levels
	  ○ discretionary access control (DAC) – restricts or allows access based on resource owner preference
	  ○ attribute-based access control (ABAC) – restricts or allows access based on attributes or characteristics
	  ○ role-based access control (RBAC) – restricts or allows access to resources based on the role of a user
	  ○ rule-based access control (RuBAC) – use a rule list to define access parameters.

1.27	**Understand physical and virtual methods of managing and securing network traffic and their application within the design of network security architecture**
	• Physical (for example businesses utilising servers, firewalls and cabling):
	  ○ software defined networking (SDN):
	  – transport layer security (TLS) (for example, used for banking websites)
	  ○ demilitarised zone (DMZ)
	  ○ air gapping.
	• Virtual:
	  ○ virtual LAN (VLAN):
	  – virtual private network (VPN) (for example, intranet, file systems, local network systems)
	  ○ virtual routing and forwarding (VRF)
	  ○ subnets
	  ○ IP security (IPSec)
	  ○ air gapping.

1.28	**Understand techniques applied and be able to install and configure software to ensure cyber security for internet connected devices, systems and networks** • Wireless security – WPA2 and WPA3 and use of end-to-end security implemented to monitor access to Wi-Fi systems. • Device security – password/authentication implemented to improve device security. • Encryption. • Virtualisation.

	• Penetration testing.
	• Malware protection.
	• Anti-virus protection.
	• Software updates and patches.
	• Multi-factor authentication.
	• Single logout (SLO).
	• Install and configure software on end user devices:
	  ○ vulnerability scanning software (for example port scanning software, device scanning software)
	  ○ anti-malware software
	  ○ firewall software.
	• Apply device hardening to remove unnecessary software.
	• Check installation and configuration on end user devices.
	• Harden devices:
	  ○ change default passwords
	  ○ set correct permissions on files and services
	  ○ apply updates and fixes
	  ○ remove unnecessary software
	  ○ apply security policies
	  ○ disable unauthorised devices.
	• Test that the installation and configuration of end user devices has been successful.
	(E4, D1, D6)

1.29	**Understand the importance of cyber security to organisations and society**
	• Organisations:
	  ○ protection of:
	  – all systems and devices
	  – cloud services and their availability
	  – personnel data and data subjects (for example, employee information, commercially sensitive information)
	  – password protection policies for users and systems
	  – adherence to cyber security legislation to avoid financial, reputational and legal impacts
	  – protection against cybercrime.
	• Society:
	  ○ protection of personal information to:
	  – maintain privacy and security
	  – protect from prejudices
	  – ensure equal opportunities
	  – prevent identity theft.

	○ individuals' rights protected under DPA 2018: – be informed about how data is being used – access personal data – have incorrect data updated – have data erased – stop or restrict the processing of data – data portability (allowing individuals to get and reuse data for different services) – object to how data is processed in certain circumstances. ○ protection against cybercrime.
1.30	**Understand techniques applied to cyber security for internet connected devices, systems and networks** • Wireless security – WPA2 and WPA3 and use of end-to-end security implemented to monitor access to Wi-Fi systems. • Device security – password/authentication implemented to improve device security. • Encryption. • Virtualisation. • Penetration testing. • Malware protection. • Anti-virus protection. • Software updates and patches. • Multi-factor authentication. • Single logout (SLO).
1.31	**Understand the fundamentals of network topologies and network referencing models and the application of cyber security principles** • Topologies: ○ bus ○ star ○ ring ○ token ring ○ mesh ○ hybrid ○ client-server ○ peer-to-peer. • Network referencing models: ○ open systems interconnection (OSI) model: – application layer – presentation layer – session layer – transport layer – network layer – data link layer – physical layer

	○ transmission control protocol/internet protocol (TCP/IP): – application layer – transport layer – network layer – network interface layer. • The minimum cyber security standards principles applied to network architecture: ○ identify – management of risks to the security of the network, users and devices: – assign cyber security lead – risk assessments for systems to identify severity of different possible security risks – documentation of configurations and responses to threats and vulnerabilities ○ protect – development and application of appropriate control measures to minimise potential security risks: – implementation of anti-virus software and firewall – reduce attack surface – use trusted and supported operating systems and applications – decommission of vulnerable and legacy systems where applicable – performance of regular security audits and vulnerability checks – data encryption at rest and during transmission – assign minimum access to users – provide appropriate cyber security training ○ detect – implementation of procedures and resources to identify security issues: – installation and application of security measures – review audit and event logs – network activity monitoring ○ respond – reaction to security issues: – contain and minimise the impacts of a security issue ○ recover – restoration of affected systems and resources: – back-ups and maintenance plans to recover systems and data – continuous improvement review.

1.32	**Understand the common vulnerabilities to networks, systems and devices, and the application of cyber security controls**
	• Missing patches, firmware and security updates:
	  ○ application of cyber security controls:
	  – patch manager software
	  – tracking network traffic
	  – test groups/devices to test security.
	• Password vulnerabilities (for example, missing, weak or default passwords, no password lockout allowing brute force or dictionary attacks):
	  ○ application of cyber security controls:
	  – minimum password requirements in line with up-to-date NCSC guidance (for example, length, special character)
	  – password reset policy.
	• Insecure basic input-output system (BIOS)/unified extensible firmware interface (UEFI) configuration:
	  ○ application of cyber security controls:
	  – review BIOS/UEFI settings
	  – update BIOS.
	• Misconfiguration of permissions and privileges:
	  ○ application of cyber security controls:
	  – testing permissions and access rights to systems
	  – scheduled auditing of permissions and privileges (for example, remove access of terminated staff).
	• Unsecure systems due to lack of protection software:
	  ○ application of cyber security controls:
	  – protecting against malware (for example, virus, worm, trojan, ransomware)
	  – update security software
	  – monitoring security software
	  – buffer overflow.
	• Insecure disposal of data and devices:
	  ○ application of cyber security controls:
	  – compliance with Waste Electrical and Electronic Equipment (WEEE) Directive 2013
	  – checking and wiping all data devices.
	• Inadequate back-up management:
	  ○ application of cyber security controls:
	  – back-up frequency
	  – application of appropriate types of back-up.
	• Unprotected physical devices:
	  ○ application of cyber security controls:
	  – install correct software.

Content area 2: Install, configure and support software applications and operating systems

What underpinning knowledge do students need?	
2.1	**Understand the values of agile methodologies and work practices** • Individuals and interactions over processes and tools. • Working software over comprehensive documentation. • Customer collaboration over contract negotiation. • Responding to change over following a plan.

2.2	**Understand the applications of agile methodologies and work practices in support of continuous innovation and development in a digital environment**
	• Scrum:
	  ○ defined roles, events, artefacts and rules
	  ○ applies daily scrums
	  ○ workloads are broken down into sprints.
	• Kanban:
	  ○ manages workloads by balancing demands with available capacity
	  ○ identifies bottlenecks in workload
	  ○ manages work using a Kanban board
	  ○ uses work in progress (WIP) limits to prevent over-commitment.
	• Dynamic systems development method (DSDM):
	  ○ fixed cost, quality and time
	  ○ uses MoSCoW in the prioritisation of scope.
	• Feature-driven development:
	  ○ breaks down development into smaller features
	  ○ plans, designs and builds by feature.
	• Crystal:
	  ○ focuses on communications and interactions between people over processes and tools.
	• Lean (7 principles):
	  ○ eliminate waste
	  ○ build in quality
	  ○ create knowledge
	  ○ defer commitment
	  ○ deliver fast
	  ○ respect people
	  ○ optimise the whole.

	• Extreme programming (XP):
	  ○ advocates frequent releases in short development cycles
	  ○ introduces check points when new customer requirements can be adopted
	  ○ uses planning and feedback loops.

2.3	**Understand the incorporation of digital technologies by organisations into key areas of business operations and the implications for digital support roles**
	• Key areas:
	  ○ finance:
	  – budget/finance dashboards
	  – invoicing processes
	  – online expense tracking
	  ○ sales and marketing:
	  – customer relationship management (CRM) systems
	  – social media management and tools
	  ○ operations:
	  – performance dashboards
	  – online ticket systems
	  ○ human resources:
	  – personnel management systems
	  – digital training
	  ○ communications:
	  – video conferencing
	  – email
	  – collaborative platforms
	  ○ research and development:
	  – access to information
	  – development environments (for example computer-aided design (CAD), integrated development environment (IDE).
	• Implications for digital support roles:
	  ○ increased demand for support due to organisational system's reliance on digital systems
	  ○ increased training needs of workforce due to reliance on digital competencies and digital skills
	  ○ increased requirement for CPD to support changing systems and technologies
	  ○ requirement to operate and maintain changing digital information systems to support the organisation to collect, store, maintain and distribute information.

2.4	**Understand the application of service functions in creating a domain within a networked environment**
	• Active directory domain services (AD DS):
	  ○ active directory – provides functionality to centrally manage and organise user and device accounts, security groups and distribution lists, contained in organisational units (OUs)
	  ○ group policy – provides functionality to create group policy objects (GPOs) which can be applied to OUs. GPOs can be applied to deploy settings and files to users' profiles and devices, based on their OU.
	• Dynamic host configuration protocol (DHCP) – a network management protocol to assign IP addresses and network configuration to a network client device.
	• Domain name system (DNS) – for the translation of hostnames to IP addresses.
	• File server and distributed file system (DFS) – to provide shared disk access and manage permissions.
	• Print server – to provide shared printer access.
	• Mail servers – manage emails to/from client mailboxes.
	• Certificate authorities – application of digital certificates to certify the ownership of a public key for use in encryption.

2.5	**Understand the applications and processes of content management system (CMS) and the methods used to identify and resolve user problems**
	• Problem/incident and request management:
	  ○ logging/raising of support requests
	  ○ tracking of request progress
	  ○ tracking open and closed tickets.
	• Knowledge management:
	  ○ identification of staff training needs (for example, use of particular software)
	  ○ collating of user support knowledge.
	• Change management:
	  ○ supporting implementation of new systems.
	• Configuration/asset management:
	  ○ tracking software licences
	  ○ responding to requests for hardware and software
	  ○ decommission or redeployment of systems/users.
	• Methods used to identify and resolve user problems:
	  ○ troubleshooting to diagnose problems:
	  – information gathering:
	  ▪ investigation of support requests
	  ▪ investigation of probable causes
	  ▪ troubleshoot issues (for example, check line speeds, check uptime and downtime)

	– problem analysis: ▪ elimination of known fixes and problems ▪ elimination of potential causes ▪ consideration of remaining possibilities – test remaining possibilities: ▪ testing and elimination of possible causes ▪ identify the appropriate solution – problem resolution: ▪ backing up data on system ▪ implementing the solution ▪ testing the solution ▪ repeating the process until required outcome ▪ documenting the cause and solution on content management system ▪ implementing security controls to mitigate against cause reoccurring.
2.6	**Understand the types of end user devices and systems where content management systems can be applied to identify and resolve user problems** • Desktop: o thick clients o thin clients. • Cloud workspaces: o free cloud workspaces o paid licensed cloud workspaces. • Mobile devices: o tablets o smartphones o wearable technology (for example, smartwatches) o e-reader. • Laptops. • Peripherals: o mouse o keyboard o monitors o printers/scanners o speakers o projectors o storage drives o magnetic reader/chip reader o smart card reader.

	• IoT:
	  ○ smart buildings:
	  – alarm systems (for example, fire, security)
	  – metres (for example, water, power)
	  – lighting
	  ○ smart devices:
	  – autonomous vehicles
	  – TVs.

2.7	**Understand the types of operating systems and how they are used in a digital support environment**
	• End user (for example, Windows, macOS, Linux):
	  ○ used on desktop PCs and laptops.
	• Mobile (for example, iOS, Android):
	  ○ used on tablets, devices and mobile phones.
	• Server (for example, Windows, Linux):
	  ○ used in client-server network environments.

2.8	**Understand the range of application types used in a digital support context**
	• Productivity software:
	  ○ word processing software
	  ○ spreadsheet software
	  ○ presentation software
	  ○ visual diagramming software.
	• Web browser.
	• Collaboration software:
	  ○ email client
	  ○ conferencing software
	  ○ voice over internet protocol (VoIP)
	  ○ instant messaging software
	  ○ online workspace
	  ○ document sharing.
	• Business software:
	  ○ database software
	  ○ project management software
	  ○ business-specific applications (bespoke)
	  ○ accounting software
	  ○ customer relationship management (CRM)
	  ○ ticket management software.
	• Development software:
	  ○ computer-aided design (CAD)
	  ○ integrated development environment (IDE).

2.9	**Understand application installation and configuration concepts in a digital support context and be able to install and configure software and systems**
	• System requirements:
	  ○ storage space
	  ○ RAM
	  ○ compatibility
	  ○ processor
	  ○ OS.
	• Hard disk drive (HDD) configuration:
	  ○ advantages:
	  – increased storage capacity
	  – lower cost
	  ○ disadvantages:
	  – high risk of damage due to moving parts
	  – greater potential to overheat.
	• Solid state drive (SSD) configuration:
	  ○ advantages:
	  – faster access
	  – faster write and rewrite speeds
	  – lower risk of damage due to no moving parts
	  – applied in devices to reduce device size (for example mobile phone, tablet)
	  ○ disadvantages:
	  – higher cost
	  – less storage capacity.
	• Network card configuration:
	  ○ advantages:
	  – efficiency
	  – highly secure
	  – runs efficiently
	  ○ disadvantages:
	  – higher cost
	  – performance lifespan.
	• Resource setup for performance optimisation.
	• Permissions:
	  ○ folder/file access for installation and operation
	  ○ user authorisation
	  ○ principle of least privilege.
	• Security considerations:
	  ○ impact to device
	  ○ impact to network
	  ○ impact on usability
	  ○ impact on the way data is stored.

	• Install and configure software and systems onto end user devices:
	  ○ remotely install an operating system and configure system settings:
	  – select appropriate boot drive and configure with the correct partitions/formats
	  – configure domain set-up
	  – configure time, date, region and language settings
	  – install additional drivers
	  – install any available updates (for example Windows updates)
	  – upgrade an existing operating system ensuring all user data is preserved.
	• Install productivity software:
	  ○ apply software updates
	  ○ install network-based software.

2.10	**Understand operating system (OS) deployment considerations in a digital support context**
	• System requirements.
	• Hardware configuration.
	• Methods of installation and deployment:
	  ○ network-based
	  ○ local (for example, CD/USB)
	  ○ virtualised
	  ○ cloud-based.
	• Boot methods:
	  ○ internal hard drive:
	  – SSD
	  – HDD
	  ○ external media drive:
	  – USB-based/solid state (for example, flash drive, hot-swappable drive)
	  ○ network-based:
	  – preboot execution environment (PXE)
	  – Netboot.
	• Partitioning:
	  ○ dynamic
	  ○ basic
	  ○ primary
	  ○ extended
	  ○ logical
	  ○ GUID Partition Table (GPT).
	• File system types:
	  ○ Extensible File Allocation Table (exFAT)
	  ○ FAT32
	  ○ New Technology File System (NTFS)
	  ○ Resilient File System (ReFS)

	○ Network File System (NFS) ○ third extended file system (ext3) ○ fourth extended file system (ext4) ○ Hierarchical File System (HFS) ○ swap partition. • File system formatting: ○ quick format: – files easier to recover – no scanning for bad sectors – less time intensive ○ full format: – full scrubbing of files – files harder to recover – full scan of bad sectors – more time intensive.
2.11	**Understand the types of deployment methods and the advantages and disadvantages of their application** • Unattended installation – requires minimal technician response due to pre-defined options being set up: • Thin imaging: ○ advantages: – used on a large scale – used on a variety of devices – ability to put out latest software for build – flexibility ○ disadvantages: – requires more maintenance – more difficult to configure. • Base image: ○ advantages: – used on a large scale – built to meet specific purpose – easier to create ○ disadvantages: – more difficult to maintain – less flexible. • In-place upgrade – upgrading an operating system without a full clean install ○ advantages: – efficient process – user profiles are not lost – simple process ○ disadvantages: – potential compatibility issues – requires operating system media or large download.

	• Manual clean install – installing an operating system with the installation media:
	  ○ advantages:
	  – most appropriate/latest version of operating system
	  – simple process
	  ○ disadvantages:
	  – may require a back-up
	  – timely process.
	• Repair installation – performing a repair installation without data loss and without upgrading:
	  ○ advantages:
	  – no loss of data
	  – no need to check compatibility
	  – may resolve operating system and application instabilities
	  ○ disadvantages:
	  – manual process
	  – may not resolve operating system and application instabilities.
	• Multi-boot – ability to boot a single device with multiple operating systems
	  ○ advantages:
	  – ability to run multiple operating systems from different manufacturers
	  ○ disadvantage:
	  – difficult to set up and maintain.
	• Remote network installation – installing an operating system from a network boot:
	  ○ advantages:
	  – physical access may not be needed
	  – takes advantage of unattended installation
	  – efficient deployment to multiple devices
	  ○ disadvantages:
	  – speed of deployment is limited to network capabilities
	  – specific network configuration may be required
	  – requirement for specific device features (for example PXE booting capabilities)
	  – significant configuration required.

2.12	**Be able to deploy software applications and operating systems remotely**
	• Gather and analyse user data to determine requirements.
	• Select and configure appropriate deployment method:
	  ○ thin imaging:
	  – gather software installer and drivers and build task sequence
	  ○ base image:
	  – install operating systems, drivers and software
	  – configure operating system, applications and drivers
	  – capture disk image.

	• Deploy operating system with chosen method. • Apply updates to operating system, applications and drivers. • Test deployment meets business requirements. • Comply with organisational safety and security policies and procedures.
2.13	**Understand the steps in creating and deploying disk images** • Creation of a base image file. • Creation of customisation or answer file. • Addition of any additional drivers and software required. • Distribution of the image. • Deployment of the image. • Updating software versions and drivers to avoid introducing vulnerabilities and instabilities.
2.14	**Understand the benefits of using image files to deploy operating systems or software** • Automation requires fewer resources. • Ensures consistency of deployment. • Reduces ongoing support costs. • Quick system restoration.

2.15	**Understand the purpose and process of system recovery and restoration**
	• System recovery:
	  ○ fixes a system in its current state
	  ○ preserves all files and folders.
	• System restoration:
	  ○ applied when system recovery fails
	  ○ reverts system back to a previous state.
	• Process:
	  ○ ensuring data is backed up
	  ○ booting in system recovery tools
	  ○ following on-screen instructions
	  ○ testing of issue to confirm resolution.

2.16	**Understand the purpose and types of corporate and internet service provider (ISP) email configurations and their applications within digital support**
	• Email configuration – server configuration of an email account used when traffic moves through a firewall or when configuring an email account set-up:
	  ○ Post Office Protocol 3 (POP3) – used to receive emails from the server to a local piece of software
	  ○ Internet Message Access Protocol (IMAP) – allows emails to be held on a mail server and received by software

	○ Simple Mail Transfer Protocol (SMTP) – used to receive emails that are sent over the internet ○ Secure/Multipurpose Internet Mail Extensions S/MIME) – used to send encrypted email messages ○ port and Secure Sockets Layer (SSL) settings – encrypted connection between the website server and the browser to improve security ○ Transport Layer Security (TLS) – successor to SSL, used to provide security for data.
2.17	**Understand the process of the configuration of on-premises and cloud-based integrated commercial provider email services:** • Ensuring alignment with corporate policy. • Configure user profiles (for example, usernames, passwords, email signatures). • Identifying and selecting: ○ provider (for example, G Suite, Microsoft 365) ○ protocol (for example, SMTP, IMAP, POP3) ○ configure mail exchange (MX) record ○ domain for incoming mail ○ domain for outgoing mail.
2.18	**Understand the purpose of remote access and its application within digital support** • Purpose: ○ facilitates work from a remote location using network resources as if connected to a physical network or a choice of multiple networks (for example, facilitates working from home due to office closure as part of a BCP). • Applications: ○ desktop sharing ○ remote support (for example, fault diagnosis, remote correction of user issues) ○ off-site working.
2.19	**Understand the role and configuration factors of a VPN in securing remote access and remote support to protect data** • Role: ○ encrypts network traffic ○ masks IP address to increase privacy. • Configuration factors: ○ settings ○ client configurations ○ server configurations ○ port and security protocols (for example, TLS, SSL) ○ encryption setting and certificates ○ authentication.

2.20	**Understand the process of configuring a simple VPN**
	• Configuration of the VPN server:
	  ○ enabling the VPN service
	  ○ configuring IP address and DNS hostnames of the VPN interface
	  ○ managing user access including authentication and permissions.
	• Configuration of the client device:
	  ○ creating the connection
	  ○ setting the destination IP address and fully qualified domain name (FQDN)
	  ○ setting permissions and conditions.

2.21	**Understand the support processes provided to end users and customers**
	• User management:
	  ○ adding users
	  ○ removing users
	  ○ accessing times.
	• Password management:
	  ○ complexity setting
	  ○ expiry
	  ○ reset on next logon.
	• Permissions and privileges:
	  ○ access to resources
	  ○ group policies
	  ○ configuring shared resources.
	• Installation and deployment of software.
	• Connection to remote resources.
	• Fault identification.
	• Issue escalation from first to third line support.
	• Knowledge management:
	  ○ documentation.
	• Known fixes.
	• SOPs.
	• Asset management.
	• Auditing.

2.22	**Be able to solve problems as they arise and apply appropriate methods in a digital support context**
	• Apply troubleshooting to diagnose problems:
	  ○ information:
	  – investigate support requests
	  – investigate probable causes
	  – troubleshoot issues.

	○ problem analysis: – eliminate known fixes and problems – eliminate potential causes – consider remaining possibilities. ○ test remaining possibilities: – test and eliminate possible causes – identify the appropriate solution. ○ apply problem resolution: – back-up data on system – implement the solution – test the solution – repeat process until required outcome is achieved – document the cause and solution on fault logging system. ○ implement actions to mitigate against the cause reoccurring.
2.23	**Be able to monitor and operate information systems** • Analyse performance of system components: ○ hardware ○ software ○ database ○ network ○ people. • Assess and monitor the appropriate security controls (for example, firewalls, anti-virus). • Monitor network performance and user traffic. • Operate and maintain assets: ○ track software licences ○ respond to requests for hardware and software ○ log and tag assets correctly. • Support users via face to face or remote access software: ○ train users in use of the system ○ organise and record user issues within a content management system ○ user password management ○ fault identification ○ issue escalation. • Record and summarise all relevant findings and actions to inform future policies and procedures: ○ logically organise all findings ○ using appropriate technical terms.

2.24	**Understand the components of version control management and its application within digital support**
	• Fresh installation:
	  ○ OS
	  ○ application software
	  ○ utility software
	  ○ licensing.
	• Patching and updating:
	  ○ system updates (for example OS updates)
	  ○ driver/firmware updates
	  ○ anti-virus/anti-malware updates
	  ○ software and applications.
	• Updates:
	  ○ installation of updates
	  ○ rollback procedures:
	  – rollback device drivers
	  ○ rollback OS update failures
	  ○ rollback updates.
	• Deployment using network tools (for example, group policy):
	  ○ locally installed
	  ○ network deployed
	  ○ testing
	  ○ release control.

2.25	**Understand the process of asset management and its application in digital support**
	• Identification and planning:
	  ○ user needs
	  ○ organisational needs
	  ○ constraints
	  ○ deployment strategies.
	• Acquisition and implementation:
	  ○ sourcing assets (for example hardware and software)
	  ○ integration into current system.
	• Operation and maintenance:
	  ○ tracking software licences
	  ○ responding to requests for hardware and software.
	• Decommissioning and redeployment:
	  ○ removing non-utilised assets
	  ○ decommissioning out-of-date systems
	  ○ management of new or leaving staff profiles.

2.26	**Understand the purpose and applications of mobile device management (MDM) and be able to configure accessories and ports of mobile devices**
	• Purpose:
	  ○ tracks and locates mobile devices
	  ○ secures mobile devices
	  ○ manages use of devices
	  ○ manages configurations:
	  – wireless data network
	  – cellular data network
	  – hotspot
	  – tethering
	  – airplane mode
	  – Bluetooth
	  – email accounts.
	• Applications:
	  ○ segregation:
	  – multiple profile options for personal and professional use
	  – management of application data
	  – compliance with organisational policies and procedures.
	• Remote management:
	  ○ remote wipe
	  ○ disabling functionalities
	  ○ restricts mobile devices
	  ○ controls app store
	  ○ restricts calling/data use
	  ○ controls back-up and synchronisation.
	• Security:
	  ○ screen lock
	  ○ encrypts device
	  ○ password enforcement
	  ○ failed login attempts/login restrictions
	  ○ multi-factor authentication.
	• Authenticator applications (for example, Google authentication, fast identity online (FIDO)).
	• Apply mobile device management (MDM) to configure mobile devices to allow:
	  ○ wireless data networks
	  ○ cellular data networks
	  ○ hotspots
	  ○ tethering
	  ○ airplane mode
	  ○ Bluetooth
	  ○ email accounts.

2.27	**Be able to explain the application and benefits of digital solutions to meet specific requirements**
	• Analyse requirements:
	  ○ access to information, services or products
	  ○ conducting transactions.
	• Identify the best application of digital solutions to meet requirements:
	  ○ digital systems (for example, content management systems)
	  ○ productivity software
	  ○ digital technologies.
	• Explain the benefits of applying the identified digital solution:
	  ○ express ideas clearly and concisely
	  ○ use appropriate level of detail to reflect audience requirements
	  ○ use technical terminology.

2.28	**Be able to operate digital information systems and tools to maintain information and delivery of a digital support service**
	• Operate information systems to collect, store, maintain and distribute information to support service delivery.
	• Process and review user feedback data on service:
	  ○ critically analyse validity of user feedback.
	• Maintain service delivery and information:
	  ○ create, action and update tickets
	  ○ communicate the status of tickets with users
	  ○ monitor and record system performance
	  ○ support users remotely by utilising remote support software.
	• Record and summarise all relevant findings and actions to inform future policies and procedures:
	  ○ logically organise all findings
	  ○ using appropriate technical terms.

2.29	**Understand the methods and tools used to train others in using digital systems and technologies, and the appropriate applications of these methods and tools**
	• Methods:
	  ○ shadowing
	  ○ desk side
	  ○ remote support
	  ○ e-learning
	  ○ VR
	  ○ AR
	  ○ smart boards
	  ○ applications (for example Kahoot!, Padlet)
	  ○ simulation.

	• Tools:
	  ○ crib sheets
	  ○ smart sheets
	  ○ webinars
	  ○ screencasts
	  ○ managed learning environments (MLE)
	  ○ virtual learning environments (VLE)
	  ○ sandboxed environments
	  ○ MOOCs.

Content area 3: Discover, evaluate and apply reliable sources of knowledge

What underpinning knowledge do students need?	

3.1	**Understand and be able to identify types of sources of knowledge that can be applied within digital support**
	• Academic publications (for example, textbooks, research journals and periodicals).
	• Supplier literature (for example, handbooks or online articles for specific devices, computers or laptops).
	• Search engines (for example, Google, Bing).
	• Websites (for example, wikis, forums, Stack Overflow, manufacturers' websites).
	• Social media (for example, company profiles for Twitter/X, Facebook and LinkedIn).
	• Blogs (for example, reviews of new technologies, opinions on topical issues in the digital sector).
	• Vlogs (for example, demonstrations, tutorials on digital technologies).
	• Professional networks (for example, digital transformation networking events/conferences).
	• E-learning (for example, MOOCs, recognised vendor qualifications, Cisco).
	• Peers (for example, colleagues, network contacts, other industry professionals).
	• Be able to identify sources of knowledge and apply factors that legitimise their use to meet requirements in a digital infrastructure context:
	  ○ identify and clarify the parameters of the requirements
	  ○ identify appropriate sources of knowledge (up to 3) (for example, search engines, blogs)
	  ○ apply the factors of reliability and validity to identified sources (for example, authority, date of publication)
	  ○ assess and review potential bias of sources
	  ○ assess and review the identified sources' appropriateness to meet the requirements.
	(E4, D1)

3.2	**Understand the factors of reliability and validity to be applied to legitimise the use of sources of knowledge** • Industry-certified accreditation (for example, Cisco certified network associate (CCNA1), Microsoft technology associate (MTA), network fundamentals). • Appropriateness. • Evidence-based: ○ citations.

	• Relevant context.
	• Credibility of author:
	  ○ affiliated to specific bodies (for example, government, industry regulators)
	  ○ reputation
	  ○ experience (for example relevant qualification in subject).
	• Target audience – produced with specific audience requirements taken into consideration (for example use of technical/non-technical terminology).
	• Publication:
	  ○ version (for example use of the current version)
	  ○ date of publication (for example if the content is outdated).

3.3	**Be able to search for information to support a topic or scenarios within digital support and corroborate information across multiple sources** • Identify and clarify the parameters of the search (for example explore the future of the digital economy, identify trends in Big Data). • Identify the sources of data that contain the required information. • Safely and securely search sources for the information required. • Corroborate sources by applying cross-referencing across multiple sources. • Apply reliability and validity factors. • Assess and review potential bias of sources. (E4, D5)

3.4	**Understand the factors of bias and be able to identify bias when using sources of knowledge in a specific digital support content**
	• Types of conscious and unconscious bias:
	  ○ author/propriety bias – unweighted opinions of the author or owner
	  ○ confirmation bias – sources support a predetermined assumption
	  ○ selection bias – selection of sources that meets specific criteria
	  ○ cultural bias – implicit assumptions based on societal norms.
	• Indicators of bias within sources:
	  ○ partiality
	  ○ prejudice
	  ○ omission.
	• Bias reduction:
	  ○ based on fact/evidence
	  ○ inclusive approach:
	  – full representation of demographics
	  – objectivity.

	• Identify bias:
	  ○ identify the types of bias (for example, confirmation, unconscious)
	  ○ identify the indicators of bias within the source
	  ○ explain clearly and concisely how bias has been created within the source
	  ○ explain clearly and concisely how bias can be avoided within sources.

3.5	**Understand and be able to demonstrate the process of critical thinking and the application of evaluation techniques and tools**
	• Process of critical thinking:
	  ○ identification of relevant information:
	  – different arguments, views and opinions
	  ○ analysis of identified information:
	  – identify types of bias and objectivity
	  – understand links between information and data
	  ○ selection of relevant evaluation techniques and tools
	  ○ evaluation of findings and drawing of conclusions
	  ○ recording of conclusions.
	• Evaluation techniques:
	  ○ formative evaluation
	  ○ summative evaluation
	  ○ qualitative (for example, interviews, observations, workshops)
	  ○ quantitative (for example, experiments, surveys, statistical analysis) benchmarking
	  ○ corroboration:
	  – cross-referencing
	  ○ triangulation.
	• Evaluation tools:
	  ○ gap analysis
	  ○ KPI analysis
	  ○ score cards
	  ○ observation reports
	  ○ user diaries
	  ○ scenario mapping
	  ○ self-assessment frameworks
	  ○ maturity assessments.
	• Apply the process of critical thinking to meet requirements:
	  ○ identify relevant information
	  ○ analyse the information
	  ○ select and apply appropriate evaluation techniques and tools
	  ○ evaluate findings
	  ○ logically organise and record conclusions.

	• Select and apply techniques and tools to support evaluation in a digital infrastructure context: o identify and clarify the parameters of the evaluation o select appropriate techniques and tools to support the evaluation o apply the selected techniques and use the appropriate tools to support the evaluation o record the findings of the evaluation for the requirement. (E1, E3, E4, M5, M6, M8, D2, D3, D4)
3.6	**Understand the functions of incident and request management systems in communicating information** • Reporting: o ticket-based: – users log issue via ticket system or email – digital support manually input details if user contacts via telephone – tracks issue trends – records internal customer satisfaction o online chat bots: – artificial intelligence (AI) responds to commonly asked questions – efficient use of digital support resource. • Recording requirements: o user/customer details o issue details o resolution o time taken. • Tracking and communicating progress: o visibility on status and escalation.
3.7	**Understand methods of communication and sharing knowledge and their application within a digital support context** • Integrated and standalone IT service management tools: o incident and problem management systems o change management systems. • Knowledge bases and knowledge management systems. • Wikis and shared documents. • Shared digital workspaces. • Telephone. • Instant messaging. • Email. • Video conferencing. • Digital signage.

	• Social media:
	  ○ organisational
	  ○ public
	  ○ personal.
	• Blogs.
	• Community forums.
	• Project management tools (for example, issue logs, Gantt charts, Kanban boards, burndown charts).
	• Policy, process and procedure documents.

3.8	**Be able to compare options of sources and rationalise the actions taken to ensure the reliability and validity of sources** • Identify the sources for comparison. • Apply the relevant reliability and validity factors to the sources. • Compare the outcomes of the validity and reliability actions. • Explain and recommend the choice of action to ensure the sources are reliable and valid, using appropriate technical terms. (E1, E3, E5, M5, D3)

4. Cyber Security

Content area 1: Apply procedures and controls to maintain the digital security of an organisation and its data

What underpinning knowledge do students need?	

1.1	**Understand the purpose of organisational information security governance**
	• To investigate, control, communicate and report cyber risks.
	• To provide a security framework for:
	  ○ defined roles and responsibilities (for example, data controller and data processor)
	  ○ organisational policies and processes (for example, data retention and deletion)
	  ○ outlining security activities (for example, evaluation of new systems and technologies).
	• To manage compliance against legislation, frameworks and standards (for example, ISO27001, data protection, freedom of information (FOI) requests).
	• To align organisational priorities and operations to mitigate against cyber threats and vulnerabilities (for example, company password complexity requirements).

1.2	**Understand the application of IT governance principles in an information security context** • Responsibility – all staff involved in information security will understand their specific roles and responsibilities (for example, asset owner, data controller and data processor). • Strategy – strategies need to be secure by design, taking into account information security constraints and future infrastructure requirements (for example, cloud-based services and data sharing) based on business requirements. • Acquisition – all purchases are evaluated, taking into account risks, benefits and costs to ensure appropriate ongoing analysis of information security and transparent decision making. • Performance – the necessary levels of preventative and remediative performance are in place to guarantee the confidentiality, integrity and availability of the information. • Conformance – IT, data and information are used in accordance with all mandatory and relevant information security legislation and regulations. • Human behaviour – technical and non-technical controls are considered in policies, processes and decisions to maintain information security.

1.3	**Understand the types and application of cyber security protection methods utilised in network infrastructure and system software**
	• Hardware:
	  ○ hardware protection – the use of server and software solutions to protect hardware and data
	  ○ device hardening – the application of updates and secure configurations to a device to increase security
	  ○ physical controls – storing hardware in secure locations, in locked cages and/or in areas with closed-circuit television (CCTV) and key card access-controlled doors.
	• Operating systems (OS):
	  ○ installation of updates or patches – the application of updates correcting security issues in older versions of the software:
	  – roll back – use of a system snapshot to aid recovery from unforeseen issues with patches or updates
	  ○ OS hardening – the removal of unnecessary accounts, functions, applications, ports and access through the application of security policies to minimise exposure to current and future threats.
	• Networks:
	  ○ segmentation and isolation – the separation of network, systems, data, devices and services to limit the ability for threat actors to traverse the network
	  ○ network monitoring – the use of tools to monitor and analyse network traffic to prevent potential threats and attacks
	  ○ network hardening – the securing of communication channels and systems between servers and devices on a shared network
	  ○ firewalls – the control and monitoring of access into and out of networks.
	• Software:
	  ○ anti-malware and anti-virus – to protect against malicious software
	  ○ authentication methods:
	  – single sign-on (SSO) – the use of one set of credentials to login to multiple services and the ability to easily manage access and control multiple systems
	  – multi-factor authentication (MFA) – the use of two or more factors to achieve authentication – something you know (for example, password), something you have (for example, token) and something you are (for example, biometric)
	  – remote monitoring and management (RMM) – the remote management of devices and performance of tasks including auditing, installing, upgrading or removing software, and obtaining diagnostic information
	  – vulnerability management and scanning – the use of an automated process to manage and identify security vulnerabilities in software infrastructure
	  – application hardening – the protection for an application against unauthorised access by eliminating vulnerabilities and increasing layers of security

	– access controls – the assignment and management of access to information: – credentials – ensuring that passwords conform to a strong password policy of sufficient length and complexity and that users are trained on how to protect their password – privileged access management (PAM) – a security measure used to control and monitor privileged users' activity – application firewalls – the control and monitoring of access and data in and out of applications – patching – ensuring that the latest security patches for installed software have been applied. • Cloud: o auditing and monitoring – detection of unauthorised or unusual behaviour through reviewing logs o access controls – the assignment and management of access to information o MFA – the use of two or more factors to achieve authentication, such as something you know (for example, password), something you have (for example, token), something you are (for example, biometric) and somewhere you are (for example, IP address location).
1.4	**Understand the potential applications of cyber security principles in network infrastructure design** • Establish the context before designing a system: o adapting a zero-trust approach at an early stage to ensure all network access requires verification o establishing the system's purpose, any requirements for operation, and what is deemed an acceptable risk o identifying the potential vulnerabilities that affect the system o considering end user behaviours and development of use cases as required o defining any supplier's role in establishing and maintaining system security o identifying organisation infrastructure from end to end, taking into account the sensitivity of data and where it is stored, manipulated and rendered o clarifying the governance of security risks and ensuring there is no ambiguity about roles and responsibilities of those involved in designing and operating a system. • Make compromise difficult: o transforming, validating and rendering data to obscure or anonymise information o reduction of the attack surface to reduce potential points of entry o having relevant security controls in place that are regularly reviewed and tested o ensuring all management and operational environments are protected from targeted attacks

	○ applying reliable and tested solutions in line with industry and organisational best practice ○ authorising and accounting for all individual operations through auditing and change control ○ designing networks and infrastructure for efficient maintenance and management (for example, access control, security patching). • Make disruption difficult: ○ ensuring systems are resilient to both attack and failure ○ designing networks and infrastructure for scalability to handle sudden and increased demand ○ identifying any potential bottlenecks that could be exploited by high load and denial of service conditions ○ identifying where availability depends on a third party and planning for the failure of that third party ○ carrying out regular testing by performing mock incident/event response scenarios to simulate a real attack ○ making it challenging for attackers to detect security rules via external penetration testing. • Make compromise detection easier: ○ gathering and analysing relevant security incident/event information and logs to identify unauthorised actions ○ ensuring alerts are in place to identify and detect known malware and to control communications ○ ensuring separation of monitoring and operational systems to allow alerting and logging to remain operational during a cyber incident/event ○ regular monitoring to understand normal behaviours, making abnormal behaviours easier to detect. • Reduce impact of compromise: ○ making use of network segmentation to limit movement of malware or threat actors across the network ○ removal of unnecessary functionality, queries or caches of data which could be compromised ○ avoiding the creation of a management bypass which could be used by threat actors to bypass security controls ○ ensuring the recovery process is straightforward and tested regularly ○ designing the network to support a separation of duties to ensure no individual or account can create a cyber incident/event either intentionally or unintentionally ○ anonymisation of data to prevent the potential loss of personal information.

1.5	**Understand the types and functions of operating systems and key components to support cyber security investigations**
	• Operating systems and devices to support them:
	  ○ client side (for example, Windows, macOS, Linux) – devices include desktop PCs and laptops
	  ○ mobile (for example, Android, iOS) – devices include tablets and mobile devices
	  ○ server side (for example, Windows, Linux) – a network operating system installed on a server.
	• Functions of operating systems:
	  ○ security – implements restrictions and controls to protect data and software (for example, zero trust)
	  ○ system performance – provides an interface between software and hardware to enable efficient performance
	  ○ error detection – detects issues and abnormalities with system software and hardware
	  ○ graphical user interface (GUI) – provides an interface for users to interact with the device
	  ○ memory management – controls operating systems' memory allocation and prevents applications reading other applications' memory
	  ○ processor management – security controls are implemented within the processor to provide additional protection (for example, protection against side-channel attacks)
	  ○ device management – the operating system may implement security controls when interfacing with hardware (for example, requiring signed drivers)
	  ○ file management – enables the operating system to manage data storage and retrieval
	  ○ program execution – enables the operating system to control how and when users can execute code and programs, and what level of permission and access those applications have
	  ○ handling input/output operations – the operating system is responsible for processing user input (for example, keystrokes on a keyboard)
	  and output (for example, graphics on a screen).
	• Key components for cyber security investigation:
	  ○ configuration files – stored in one location on a Linux system each containing settings and instructions for applications and processes
	  ○ registry – a database of configurations for a Microsoft Windows based system that manages values for installed hardware and software
	  ○ logs – used to monitor network performance and traffic flow
	  ○ library/preferences – stored in one location in macOS, the system preference files contain rules for the system and applications

	○ file system – stores, manages and organises data on the storage disk – this can differ depending on the operating system (for example, New Technology File System (NTFS), File Allocation Table 32-bit (FAT32), extended File Allocation Table (exFAT), Apple File System (APFS), forth extended file system (ext4)) ○ processes – provides real-time information on a Microsoft Windows based system.
1.6	**Understand the role of physical and virtual server types** • Server (for example, Linux, Windows Server) – applied to client-server environments: ○ physical servers – running applications directly on physical hardware, allowing full access to the hardware ○ virtualisation: – virtual servers – allows a single piece of hardware to run multiple operating systems and software at the same time, in isolated environments – containers – virtualisation of software and application packages which are separated and isolated from other packages and the underlying operating system for added security and portability using only packages required for the software to function.
1.7	**Understand the purpose and core processes of IT service management (ITSM)** • Purpose – to manage the end-to-end delivery of IT services to customers. • Core processes: ○ service request management – handling queries from customers and tracking the resolution of incidents/events (for example, reporting of a potential cyber incident/event to the service desk) ○ knowledge management – maintaining documentation, ensuring it is up to date and relevant (for example, documented and standardised hardened builds) ○ IT asset management – using tools (for example, configuration management database (CMDB)) to keep track of hardware, software, systems and IT configurations (for example, history, location, owner) ○ problem and incident management – understanding the root causes and co-ordinating, responding to, and resolving incidents/events as they occur (for example, standardised incident management processes and procedures in place for cyber incidents/events) ○ change management – ensuring that changes to IT services are agreed upon by stakeholders and recorded (for example, introduction of a new firewall rule).

1.8	**Understand the application of the Information Technology Infrastructure Library (ITIL®) service lifecycle** • Service strategy – aligns to business objectives to ensure that the service is fit for purpose and fit for use. • Service design – design of services and all supporting elements for introduction into the live environment, ensuring that people, processes, products and partners are all considered. • Service transition – building and deploying services and ensuring that any changes are managed in a coordinated way. • Service operation – fulfilling requests, resolving failures, fixing problems and carrying out routine operational tasks. • Continual service improvement – continually improving the effectiveness and efficiency of IT processes and services.
1.9	**Understand the application of cyber security principles associated with the transmission of digital information** • Identification of the security requirements of the data: o making use of the Confidentiality, Integrity and Availability (CIA) triad – confidentiality, integrity and availability applied to develop security. • Prevention of eavesdropping of data whilst in transit: o making use of asymmetric encryption techniques. • Authentication and verification of data: o making use of aspects of cryptography – integrity, authenticity, confidentiality, non-repudiation.
1.10	**Understand the role of frameworks and standards to support an organisation's information security management system (ISMS)** • Role of ISMS – used to create policies (for example, information security policy, acceptable use policy) to ensure an organisation is compliant with security and privacy standards. • Role of frameworks: o Control Objectives for Information and Related Technologies (COBIT) – used in helping organisations to develop procedures and internal frameworks for governance and management of IT systems o Service Organisation Controls (SOC 2) – used in assessing an organisation's security, availability, processing integrity, confidentiality and privacy controls o National Institute of Standards and Technology (NIST) – used by organisations to help them understand ways to improve how they manage cyber security risks.

	• Role of standards:
	  ○ ISO 27000 information security management – a series of standards and best practice guides for information security management:
	  – ISO 27001 – used to establish, implement, maintain and continually improve an information security management system within an organisation
	  ○ ISO 35800:2015 – a framework for governance of IT for an organisation
	  ○ National Cyber Security Centre (NCSC) Cyber Essentials and Cyber Essentials Plus – a government-backed scheme that supports organisations to protect against cyber-attacks and provides accreditation to organisations
	  ○ Payment Card Industry Data Security Standard (PCI DSS):
	  – designed to reduce payment card fraud by increasing security controls for organisations that store, process or transmit credit card data.

1.11	**Understand the purpose and importance of a disaster recovery plan (DRP) to support risk management**
	• Purpose – a formal document that details instructions on how to respond to unplanned incidents/events, including natural disasters, power outages, cyber-attacks and any other disruptive events.
	• Importance:
	  ○ minimises mean time to recovery (MTTR)
	  ○ minimises interruptions to normal operations
	  ○ limits the extent of disruption and damage
	  ○ minimises the economic impact of the interruption
	  ○ establishes alternative means of operation in advance
	  ○ enables a prompt restoration of service
	  ○ supports the identification of potential issues (for example, lack of staff training).

1.12	**Understand the implementation of a DRP to support risk management**
	• Defining the scope of the incident/event:
	  ○ environmental or technical impact – determining the nature of the disaster
	  ○ organisational impact – identifying whether the disaster impacts all users across the organisation
	  ○ departmental impact – identifying how departments are impacted by the disaster
	  ○ individual impact – identifying how individuals are impacted by the disaster.
	• Gathering relevant information:
	  ○ historic outage details
	  ○ inventories of hardware, software, networks and data
	  ○ contact information for any parties involved.

	• Risk-assessing – identifying threats and vulnerabilities in assets and determining the likelihood of occurrence and impact on business-as-usual operations.
	• Creation of the plan:
	  ○ identifying the resources required for the DRP:
	  – systems, equipment and utilities required to continue business as usual operations
	  – staff contact details and documented roles and responsibilities
	  – financial commitment required to implement the DRP in response to incident/event.
	• Plan approval:
	  ○ sign off by appropriate parties.
	• Testing of the plan:
	  ○ identifying scope of the test and required resources
	  ○ determining frequency of the test
	  ○ conducting the test
	  ○ reviewing and documenting outcome of the test
	  ○ amending the plan based on review as required.
	• Continuous improvement:
	  ○ internal and external auditing of plan.
	• Review existing control measures through a gap analysis:
	  ○ identify changes that have occurred since controls were implemented
	  ○ identify any missing requirements.
	• Assess effectiveness of existing controls.
	• Identify areas and required adaptions for continuous improvement to mitigate vulnerabilities (for example, an incident detected in networked equipment, updating devices with the latest releases of security software, penetrating testing).
	• Record and communicate suggested areas for continuous improvement.
	(M10, D3)

1.13	**Understand the purpose and types of preventative controls implemented to protect an organisation's information**
	• Purpose – to prevent unauthorised access or tampering, or mitigate against environmental incidents/events through the implementation of effective controls.
	• Physical controls:
	  ○ specialist locks:
	  – anti-picking
	  ○ barriers:
	  – fencing
	  – bollards
	  – gates
	  – cages

	○ flood and fire defence systems. • Managed entry access controls: ○ manned reception desk ○ security guards ○ restricted door controls ○ card readers. • Biometric: ○ facial recognition ○ fingerprints. • Video/closed-circuit television (CCTV). • Pin/passcodes. • Technical controls: ○ firewalls ○ allow and deny control lists ○ sandboxing ○ device hardening: – changing default passwords – setting correct permissions on files and services – applying updates and fixes – removing unnecessary software – application of security policies – disabling unauthorised devices (for example, USB flash drives). • Procedural controls: ○ separation of duties and relevance of role-based access control (RBAC).
1.14	**Understand the purpose and types of corrective controls implemented to protect an organisation's information** • Purpose – to limit the extent of damage and reoccurrence. • Corrective control techniques: ○ physical controls: – fire suppression: ▪ sprinklers ▪ extinguishers. ○ gas suppression: – inert – chemical ○ technical controls: – patching – disconnecting infected systems – quarantining a virus ○ procedural: – standard operating procedure (SOP) (for example, actions taken when a fire is identified) – DRP.

1.15	**Understand the purpose and types of compensating controls implemented to protect an organisation's information**
	• Purpose – provides a safeguard against primary control failure.
	• Compensating control techniques:
	  ○ physical controls:
	  – segregation of duties – sharing of responsibilities to ensure greater security measures are in place
	  – log management and auditing (for example, key code access) – storing a log of which individuals enter a location
	  ○ technical controls:
	  – encryption
	  ○ procedural controls:
	  – mandatory and regular cyber awareness training
	  – regular testing of controls (for example, simulated attacks)
	  – SOPs (for example, environmental control monitoring).

1.16	**Be able to protect personal, physical and environmental security**
	• Review the potential security risk:
	  ○ gather information from systems and users (for example, security events, logs).
	• Select and apply appropriate security controls in accordance with the risk:
	  ○ preventative controls
	  ○ corrective controls
	  ○ compensating controls.
	• Comply with relevant regulatory and organisational policies and procedures as required (for example, Data Protection Act 2018, data protection policy).

1.17	**Understand the purpose and characteristics of cryptography**
	• Purpose of cryptography – applying encryption or hashing to ensure the secure and authenticated transmission of data.
	• Characteristics of cryptography:
	  ○ encryption – reversible form of cryptography (for example, using public or private keys)
	  ○ confidentiality – ensuring only the intended recipients of information can decrypt the data with symmetric or asymmetric encryption
	  ○ authenticity – enables the recipient of data to verify the sender using digital signatures (asymmetric encryption)
	  ○ hashing – non-reversible form of cryptography using an algorithm to provide a fixed length output (for example, password hashing)
	  ○ integrity – ensures data cannot be modified in transit by utilising hash-based message authentication code (HMAC).
	• non-repudiation – used in conjunction with other aspects of cryptography to provide a guarantee of the author of a message using a message authentication code (MAC).

1.18	**Understand the purpose, features and types of digital certificates**
	• Purpose of digital certificates – an electronic signature that proves the authenticity of a device, server or user through the use of asymmetric cryptography.
	• Features of digital certificates:
	  ○ name of certificate holder – company, server, device
	  ○ unique serial number – a unique number assigned only to one certificate
	  ○ expiration date – the date after which the certificate is no longer valid
	  ○ certificate holder's public key – used for encrypting and decrypting digital signatures and messages in association with public key infrastructure
	  ○ issuer's signature – identification information of the issuing authority.
	• Types of digital certificates:
	  ○ server side – allows a client to verify the authenticity of a server
	  ○ client side – allows a client to authenticate to a server
	  ○ code signing – allows an operating system to verify the author and integrity of software.

1.19	**Understand the purpose of certificate management tools**
	• Monitors expiration dates.
	• Revokes certificates, if required, before the expiration date.
	• Performs auto renewal of expired certificates.
	• Creates, signs and issues certificates:
	  ○ auditing of certificates – validating a certificate is deployed/removed as required
	  ○ diagnosis to confirm that appropriate certificates are deployed when resolving issues.

1.20	**Understand the process for the generation of a digital certificate** • Generation of a public and private key. • Generation of a certificate signing request (CSR). • Issuing and signing of certificate by a trusted certificate authority (CA). • Installation of certificate on client/server device.

1.21	**Understand the purpose of legislation in relation to the cyber security industry**
	• Data Protection Act (DPA) 2018:
	  ○ imposes obligations to:
	  – protect personal data against cyber attacks
	  – detect security events
	  – minimise the impact of an incident/event.

	• Investigatory Powers Act 2016:
	  ○ collates all powers of law enforcement, security and intelligence agencies to obtain information and data communications
	  ○ updates the ways the investigatory powers are authorised and overseen
	  ○ makes sure investigatory powers meet digital requirements.
	• Human Rights Act 1998:
	  ○ protects human rights from exploitation
	  ○ all public authorities or bodies exercising public functions must follow the act.
	• Telecommunications (Security) Act 2021:
	  ○ introduces duties for providers of public electronic communications networks and services to:
	  – prevent the occurrence of risks through identifying and reducing the chances of security compromises occurring
	  – mitigate and remedy any effects in the event of a security compromise
	  – inform network or service users of the security compromise.
	• Computer Misuse Act 1990:
	  ○ criminalises the unauthorised interference with computers, including:
	  – unauthorised access to computer material
	  – unauthorised access to computer material with intent to commit a further crime
	  – unauthorised modification or deletion of data
	  – making, supplying or obtaining anything that can be used in computer misuse offences.
	• Freedom of Information Act 2000:
	  ○ protects certain security public authorities (for example, NCSC) and exempts them from having to disclose information.
	• Network and Information Systems Regulations 2018 (UK):
	  ○ aims to establish a common level of security for network and information systems
	  ○ applies to 2 groups of organisations:
	  – operators of essential services (OES)
	  – relevant digital service providers (RDSPs)
	• Official Secrets Act 1989:
	  ○ protects the disclosure of information relating to security or intelligence.
	• Wireless Telegraphy Act 2006:
	  ○ law relating to the regulation of wireless transmitting devices in the UK
	  ○ aims to make it a criminal offence to obtain information from wireless networks without prior permission
	  ○ prohibits the misuse of wireless technology (for example, intercepting and disclosing information).

1.22	**Understand the key features of ethical codes of conduct within cyber security**
	• UK Cyber Security Council Code of Ethics:
	  ○ credibility:
	  – maintain the highest standards in service delivery, advice and conduct
	  – act in ways that are accountable and ethical
	  ○ integrity:
	  – show honesty and integrity in the conduct of activities and services
	  – demonstrate compliance with legislation and regulations
	  ○ professionalism:
	  – uphold and improve the professionalism and reputation of the cyber security sector by sharing experiences, opportunities, techniques and tools
	  – promote and advance public awareness and understanding of cyber security and its benefits
	  – apply evidence-based practices
	  – correct any false or misleading statements about the industry or profession
	  ○ responsibility and respect:
	  – take responsibility
	  – demonstrate good practice with regards to the safeguarding of data and information
	  – declare any conflicts of interest
	  – champion equality of opportunity, diversity and inclusion and support human rights, dignity and respect.
	• British Computer Society (BCS) code of conduct:
	  ○ you make IT for everyone:
	  – maintain professionalism while sharing information
	  ○ show what you know, learn what you do not:
	  – only undertake work within your professional competence
	  – continuously develop your knowledge and skills
	  – develop a good understanding of legislation
	  – remain respectful and ethical
	  ○ respect the organisation or individual you work for:
	  – conduct duties demonstrating due care and diligence
	  – show professional responsibility
	  – do not disclose any information for personal gain
	  – do not take advantage of the inexperience of others
	  ○ keep IT real; keep IT professional; pass IT on:
	  – uphold the reputation of the profession
	  – help to improve professional standards
	  – act with integrity and respect
	  – encourage and support members.

1.23	**Understand the definitions of core terminology in cyber security**
	• CIA triad – a model that forms the basis for security systems and consists of 3 core components:
	  ○ confidentiality – the access and modification of data is restricted to authorised users
	  ○ integrity – data is maintained in appropriate form without unauthorised modification
	  ○ availability – authorised users are able to access data as required.
	• Identification, authentication, authorisation and accountability (IAAA) – a concept to explain access control in cyber security:
	  ○ identification – a unique form of identity bespoke to the individual user (for example, full name, username, employee number)
	  ○ authentication – the process of verifying a person's identity:
	  – methods of authentication:
	  ▪ single factor authentication
	  ▪ multi-factor authentication (MFA)
	  ○ authorisation – the process of attributing and allowing permissions for users through access control models
	  ○ accountability – assurance of actions being performed by a user are traceable to confirm sender identify and proof of receipt
	  ○ access controls methods – restricts or allows access to areas of a business (for example, mandatory access control (MAC))
	  ○ defence in depth – the process of layering security mechanisms to provide protection to a system should one layer fail or be bypassed
	  ○ reliability – a system or component capability to function under specified conditions for a specified period of time
	  ○ assurance – analysis of security requirements of IT systems, policies and procedures to confirm that security requirements have been met.

1.24	**Be able to manage and assess the validity of security requests**
	• Assess the validity of the security request, considering:
	  ○ origin of request
	  ○ reason for request
	  ○ status and permissions of requestor (for example, staff member, external stakeholder)
	  ○ sensitivity of request (for example, exposure of personal data)
	  ○ any new risks that will be introduced as a result of the security request
	  ○ manage security request in line with regulatory requirements.
	(D4)

Content area 2: Propose remediation advice for a security risk assessment

What underpinning knowledge do students need?	

2.1	**Understand the purpose and application of compliance principles in computer forensics**
	• Purpose:
	  ○ a method of investigating and analysing digital devices and computer networks to gather legitimate evidence for presentation to an appropriate body (for example, law enforcement).
	• Application of compliance principles:
	  ○ identification – identification of what evidence is present and where and how it is stored
	  ○ preservation – avoidance of tampering and contaminating evidence, either accidentally or intentionally, by isolating, securing and preserving digital evidence in a chronological order in line with legal retention periods
	  ○ analysis – reconstructing fragments of data and drawing conclusions based on evidence
	  ○ documentation – recording of all visible data and documentation of the investigation
	  ○ presentation – presentation of all findings to an appropriate body (for example, law enforcement) for further investigation.

2.2	**Understand types of potential cyber security threats and methods of identification and be able to identify and categorise threats, vulnerabilities and risks**
	• Social engineering:
	  ○ phishing – a fraudulent message designed to trick large numbers of individuals into revealing sensitive information or to deploy malicious software:
	  – message may be sent from a public email domain or a spoofed email address
	  – the domain name may be misspelt
	  – the email may be poorly written or contain spelling mistakes
	  – the email may include infected attachments or suspicious links
	  – the message may create a sense of urgency
	  ○ spear phishing – a difficult-to-detect, targeted email attack sent to specific individuals to trick them into clicking or downloading malicious software or initiating an undesired action (for example, bank transfer):
	  – identification methods are similar to phishing but, as the attack is more sophisticated and personalised, it is more difficult to detect

	○ vishing – fraudulent phone calls or voice messages purporting to be from reputable companies to induce individuals to reveal personal information: – may request confidential information (for example, date of birth, credit card numbers, National Insurance number) – may use a demanding tone to push victims to reveal information (for example, a memorable word used as part of multi-factor authentication (MFA)) – call may be unexpected and unplanned (for example, claiming to be from a governmental department such as His Majesty's Revenue and Customs (HMRC)) ○ smishing – fraudulent text messages posing to be from reputable companies trying to persuade individuals to reveal personal information: – use of unknown or hidden numbers – message may appear to come from a well-known institution (for example, a bank requesting personal or financial information) – may include suspicious links (for example, offering a rebate or a refund) ○ shoulder surfing – criminal practice using observation techniques to get information (for example, pin numbers, passwords or other personal data): – individuals standing too close or looking over someone's shoulder – dumpster diving – a technique used to retrieve information from disposed items that could be used to carry out an attack – use of discarded personal information – denial-of-service (DoS) – a malicious attempt to overwhelm an online service and render it unusable – identification through monitoring and analysis of network traffic – degraded network performance – increased traffic to network – multiple requests from same IP address – service outages/website inaccessible. • Distributed denial-of-service (DDoS) – involves many computers attacking the same online service at the same time to render it unusable: ○ identification through monitoring and analysis of network traffic: – degraded network performance – increased traffic to network – multiple requests from same IP address – service outages/website inaccessible – zero-day attack – exploited by the attacker before the developer can release a patch ○ identification through monitoring and analysis of network traffic: – statistics provided by anti-malware vendors – unusual scanning activity

	– monitoring digital signatures using machine learning to identify previous attacks – monitoring interaction with existing software and systems to identify and manage malicious activity. • Malware: o virus – spreads between networked devices and causes damage to data and software: – appearance on scanning reports – potentially reduced or inhibited performance of device o adware – unwanted programme that displays ads on computers and mobile devices: – unexpected change in web browser home page – web pages not displaying correctly – slow device performance – device crashing – reduced internet speeds – redirected internet searches o ransomware – malicious software designed to block access, delete or amend a computer system or data until a sum of money is paid: – inaccessible data – appearance on malware detection reports – user alerts o trojan – downloads onto a computer disguised as a legitimate programme or hidden within an application: – appearance on scanning reports – potentially reduced or inhibited performance of device o botnet – network of computers or internet-connected devices under a threat actor's control: – slow internet access – device crashing – problems with shutting devices down o spyware – hides on devices, monitors activity and steals sensitive information (for example, bank details, passwords): – appearance on scanning reports – potentially reduced or inhibited performance of device. • Password attack – attempts by threat actors to determine a password: o brute force – a computer programme that works through all possible letter, number and symbol sequences character by character, until hitting the correct combination: – increased network activity – failed login attempts from the same IP address – unusual user behaviour

	○ dictionary attack – a computer program that uses common words and phrases to work out a password: – increased network activity – failed login attempts from the same IP address – unusual user behaviour ○ man-in-the-middle – attackers attempting to intercept communications: – web browser security warnings – unexpected or repeated disconnections. • Identify and categorise threats, vulnerabilities and risks: ○ identify potential threats, vulnerabilities and risks ○ calculate the likelihood and severity of the identified threats, vulnerabilities and risks ○ analyse and categorise the priority based on level of risk.
2.3	**Understand types of threat actors and motivations for an attack, and the importance of threat intelligence** • Threat actors – a person, group or entity that performs a cyber-attack: ○ cyber criminals – use of ransomware, social engineering or malicious software to steal sensitive information to result in financial gain ○ insiders – current or past employees use authorised access to gain company information to seek revenge or financial gain ○ terrorist organisations – cause disruption to organisations to bring awareness to their cause (for example, recruitment purposes, propaganda, financial gain, political reasons) ○ nation state – steal sensitive information to influence populations and damage critical infrastructure for political gain ○ hacktivists – expose or draw awareness to government agencies or businesses and are motivated by using their findings 'for good' ○ script kiddies – novices who are experimenting in the field will conduct attacks for the challenge and thrill of breaking into networks illegally. • The importance of threat intelligence – the process of gathering critical information to help analyse and prioritise potential threats: ○ enables the identification of previously unknown or emerging threats ○ provides knowledge of threat actors and their motivations ○ supports decision making to mitigate threats quickly and effectively.

2.4	**Understand the stages and application of a risk assessment and be able to scope, document and evaluate results of vulnerability assessments**
	• Identification of vulnerability:
	  ○ analysis of scans and logs to check for anomalies.
	• Analysis of vulnerability:
	  ○ checking if the vulnerability can be exploited and assessing the severity.
	• Identification of risks associated with vulnerabilities:
	  ○ prioritisation of risks.
	• Remediation:
	  ○ updating or removing affected hardware/software.
	• Mitigation:
	  ○ application of appropriate countermeasures
	  ○ close down mitigated vulnerabilities
	  ○ escalate vulnerabilities that still pose a threat.
	• Identify the scope of vulnerability assessment information:
	  ○ identify the systems, services and networks that are in scope for the assessment
	  ○ identify access requirements
	  ○ identify the vulnerabilities that the systems will be tested against.
	• Evaluate the results of the vulnerability assessment information:
	  ○ classify the risks posed by any identified vulnerabilities
	  ○ determine the business impact the vulnerability could have on an organisation (for example, loss of data).
	• Document and organise results of the vulnerability assessment.

2.5	**Understand the application of the Common Vulnerabilities and Exposures (CVE) technique to evaluate the results of a vulnerability assessment**
	• Identification of known CVEs published (for example, published by vendor, penetration tester).
	• Research into CVE:
	  ○ performance of a risk assessment based upon the Common Vulnerability Scoring System (CVSS) scores – a score which ranks vulnerabilities on a scale of 0 to 10.0 depending on their impact, ease of exploitation and severity
	  ○ identification of systems affected
	  ○ identification of mitigations.
	• Implementation of suggested mitigations.

2.6	**Understand factors to consider and be able to make recommendations for mitigations based upon the evidence provided by vulnerability assessment tools**
	• Potential risks and impact on business, operations and infrastructure.
	• Mitigating circumstances leading to the vulnerability.
	• Cost of implementing or not implementing the recommendations.
	• Type and severity of the vulnerability.
	• Availability of resources:
	  ○ people
	  ○ finances
	  ○ technology.
	• Timeframes – obligations for reporting and response time based upon findings.
	• The scope and priority based upon the CVE score.
	• Potential mitigation responses.
	• Results from a proof-of-concept (PoC) simulation – completed to confirm flaws in a network.
	• Document recommendations logically and coherently and communicate using appropriate terminology to required audiences.

2.7	**Understand the potential impacts that an exploited vulnerability might have on an organisation**
	• Damage to property and resources – damage to property, infrastructure and resources caused by safety risks or vulnerabilities within control systems.
	• Financial loss – loss of income due to inability to continue or perform normal business functions.
	• Reputational damage – harm to an organisation's public image and loss of customer trust following exposure of sensitive or personal information.
	• Fines or prosecution – fines by a court or regulating body due to non-compliance (for example, a fine from the Information Commissioner’s Office (ICO) because of a data breach).
	• Operational disruption – an organisation's inability to conduct its day-to-day operations and perform normal business functions.
	• Harm to employees:
	  ○ physical harm – harm caused to an individual due to vulnerabilities in control systems (for example, interference with fire defence systems)
	  ○ psychological harm – exposure of an individual’s sensitive data resulting in psychological harm.
	• Identity theft – an employee's personal information being stolen because of a vulnerability (for example, taking out loans or credit cards in their name).

2.8	**Understand the purpose of risk assessments on network infrastructure** • Host based – identifies vulnerabilities in workstations, servers or other network hosts and provides visibility into configuration settings and patch history. • Network based – identifies potential network security attacks and vulnerable systems on networks. • Wireless based – identifies rogue access points and confirms that a company's network is securely configured. • Application based – identifies known software vulnerabilities and misconfigurations in network or web apps (for example, structured query language (SQL) injection).
2.9	**Understand the strengths and weaknesses of vulnerability assessment tools** • Infrastructure scanners – applied to host, network and wireless infrastructure: o strengths: – identifies missing patches – identifies unsupported systems – discovers weak passwords – provides exposure of services – discovers missing hardening measures – identifies incorrect access controls o weaknesses: – does not protect against malicious attacks – only discovers threats that have previously been identified – vendor fixes can take a long time to implement – potential for inaccuracy of results – potential to affect services on devices during scans. • Web application scanners – applied to applications and network infrastructure: o strengths: – automatic scanning process – discovers SQL injection – identifies if authentication is not functioning correctly – highlights exposure of data – identifies incorrect access controls – discovers vulnerable third-party use – identifies weak or unencrypted communications o weaknesses: – identifies a vulnerability when one is absent (for example, false positives) – fails to identify a vulnerability when one is present (for example, false negatives) – impacts on system resources during scanning process – only discovers threats that have previously been identified.

	• Software scanners – applied to applications:
	  o strengths:
	  – discovers missing updates
	  – identifies missing patches
	  – performs vendor-specific checks
	  o weaknesses:
	  – regular updates are required
	  – identifies a vulnerability when one is absent (for example, false positives)
	  – fails to identify a vulnerability when one is present (for example, false negatives)
	  – difficult to identify the impact the vulnerability will have on the business and infrastructure.

2.10	**Understand types of potential risks within an organisation and the associated management approaches**
	• Compliance risks – not implementing or adhering to policies and procedures:
	  o monitoring and updating of processes and procedures
	  o controls to monitor compliance
	  o exception reports – a report that highlights to management the potential upcoming issues before they become major problems (for example, software support about to expire).
	• Safety risks – harm to individuals, property or the environment:
	  o consistent checks for human error
	  o auditing of maintenance processes.
	• Information security risks – an incident/event that results in business information being lost, stolen, copied or otherwise compromised:
	  o control measures for data (for example, access controls)
	  o monitoring of network traffic
	  o device management (for example, restricted USB access)
	  o regular and effective information security training.

2.11	**Understand potential threats and mitigation approaches to prevent privacy breaches**
	• Social engineering:
	  o raising awareness of recent cyber issues.
	• Unmanaged devices:
	  o introduction of company policies to ensure unmanaged devices aren’t used.
	• Providing staff with secure devices.
	• Untrained staff:
	  o undertaking training of staff
	  o production of SOPs.
	• Insider threats:
	  o implementing appropriate access controls
	  o monitoring unusual activity

	○ segregation of duties. • Insecure unpatched applications: ○ ensuring all patches and updates are installed. • Third-party risk (for example, a cloud organisation handling data): ○ undertaking due diligence checks of suppliers prior to use. • Improper disposal of devices: ○ securely wipe devices prior to disposal ○ adhering to relevant legislation (for example, Data Protection Act 2018).
2.12	**Understand the purpose of measures used in risk management to assess the impact of threats and vulnerabilities** • Recovery time objective (RTO) – a way of measuring how much time it takes after the disaster has occurred to recover systems to an acceptable operational state. • Recovery point objective (RPO) – a way of measuring loss tolerance and how much data can be lost or manually recovered. • Mean time between failures (MTBF) – a way of anticipating the likelihood of an asset failing or how often a failure may occur. • Mean time to detect (MTTD) – a way of measuring how efficient the detection capabilities are. • Mean time to recovery (MTTR) – a way of measuring the average time it takes to maintain and restore a failed system.
2.13	**Understand the factors to consider in the identification and classification of critical systems** • Single point of failure within an organisation's system – the potential risks posed by a flaw in the design, implementation or configuration of a system, where a single point is depended upon. • Mission essential functions of an organisation – functions that must be continued throughout or resumed rapidly, after a disruption to normal operations.
2.14	**Understand the potential factors involved in threat assessment to support information security** • Environmental: ○ power failure ○ power spikes ○ natural disasters ○ fire ○ equipment failure ○ flooding. • Manmade: ○ internal: – malicious or inadvertent activity from employees – human error – misconfigured firewall settings

	○ external: – malware – attack – social engineering – terrorism.
2.15	**Understand the application of qualitative and quantitative approaches and tools for the analysis of threats and vulnerabilities** • Approaches: ○ qualitative – applied to business risks through non-numeric methods: – determination of severity of threats and vulnerabilities using red, amber, green (RAG) rating: – red – high risk requiring immediate action – amber – moderate risk that needs to be observed closely – green – low risk with no immediate action required ○ quantitative – applied to business risks through numerical methods: – determination of the effects of threats and vulnerabilities using numerical methods (for example, cost overrun, resource consumption) – calculation based on single loss expectancy (SLE) x annual rate of occurrence (ARO) = annual loss expectancy (ALE) – use of CVSS – a score which ranks vulnerabilities on a scale of 0 to 10.0 depending on their impact ○ tools: – fault tree analysis – a graphical representation used to analyse the causes of a system level failure – failure mode, effects and criticality analysis (FMECA) – a structured method used to assess the causes of failures for a product or process and the effect on production, safety, cost and quality – CCTA Risk Analysis and Management Method (CRAMM) – a risk analysis methodology that comprises 3 stages; the first 2 scope and evaluate the risk and the third recommends counter measures – Factor Analysis of Information Risk (FAIR) – a model for understanding, analysing and quantifying cyber risk and operational risk in qualitative terms.
2.16	**Understand the process and application of a security risk assessment and be able to conduct a security risk assessment on a device connected to a local area network (LAN)** • Process: ○ identification of potential security risks that might occur ○ assessment of the security risks using a scoring matrix: – likelihood – probability of a security risk happening – severity– impact of an incident/event on the organisation – calculation of the overall risk rating – likelihood x severity = risk score/RAG rating

	○ assessment of the asset value versus the potential mitigation controls ○ control of the security risks – responses must be proportionate to risk and value ○ record of the findings. • Regular review and test of the controls. • Application – performing regular security risk assessments using internal or external auditors to cover key business areas (for example, in-house computer systems and third-party suppliers). (E3, E4, M5, M6, M8)
2.17	**Understand the stages and application of penetration testing in vulnerability assessments** • Planning and scoping – identification of rules of engagement, timings, legalities and contractual obligations. • Reconnaissance – investigation of business and operations with the purpose of gathering information about the system (for example, network topology, operating systems, applications). • Scanning – utilisation of various tools to identify open ports and network services on the system. • Vulnerability assessment – scanning of the system to identify potential vulnerabilities and determine whether they can be exploited to gain access. • Exploitation – attempts are made to exploit the vulnerability and access the system. • Reporting – creation of documentation that details the findings of the penetration test and provides recommendations to fix or mitigate any vulnerabilities found in the system.
2.18	**Understand the types of risk response utilised within cyber security** • Accept – the impact of the risk is deemed acceptable when there is no mitigation available, or the relevant mitigation has been applied and there is still a risk remaining. • Transfer – the outsourcing of the risk to another party to manage, lower or offset the risk. • Avoid – changing the scope of a project or system to avoid the identified risk. • Mitigate – reducing the severity or likelihood of the identified risk by implementing relevant controls or measures.

2.19	**Understand the stages and process of incident/event management and be able to document incident/event and exception information in an appropriate format**
	• Identification of the incident/event (for example, via service desk, phone calls, emails, SMS, live chat messages).
	• Logging of the incident/event:
	  ○ manual (for example, raising a ticket):
	  – contact details of the individual raising the ticket
	  – date and time of the incident/event
	  – description of the incident/event
	  ○ automatic (for example, raised by a monitoring system):
	  – date and time of the incident/event
	  – description of the incident/event.
	• Management of the incident/event:
	  ○ creation of incident/event ticket and allocation of ticket number, to allow for tracking
	  ○ assignment to relevant personnel (for example, technician):
	  – based on relevant expertise, level of system access and seniority of personnel
	  – breakdown of task as required (for example, into sub-activities)
	  ○ categorisation of the incident/event:
	  – based upon the disruption that may be caused to the business or a service (for example, disruption to one business area or one area of the network, or disruption to all business areas and all areas of the network).
	• Prioritisation of the incident/event:
	  ○ high risk requiring immediate action
	  ○ moderate risk that needs to be observed closely
	  ○ low risk with no immediate action required
	  ○ service level agreement (SLA) management and escalation:
	  – conformance and compliance with SLA of task
	  – variance against SLA escalated to appropriate personnel
	  ○ escalation:
	  – determine whether the incident/event needs to be escalated within or outside of the IT team
	  – escalate the incident/event to the relevant authorities as appropriate
	  – crimes – reported to the police
	  – data breaches – reported to the ICO.
	• Resolution of the incident/event:
	  ○ temporary workaround or permanent solution.
	• Closure of the incident/event:
	  ○ confirmation of incident/event resolution
	  ○ confirmation from user, if applicable

	○ population of incident/event report, summarising: – executive summary: ▪ a high-level overview to management summarising the report content without too many technical details – discovery: ▪ discovery of the incident/event – the investigation that has been undertaken ○ impact: – the effect the incident/event has had on the business ○ mitigation: – the actions that have been taken ○ recommendations: – the suggested measures to reduce the chances of a repeat incident/event ○ ongoing risks: – details of any outstanding risks. • Document incident/event and exception information: ○ gather information relevant to incident/event or exception ○ complete management reports in line with organisational policies and procedures: ○ incident/event report ○ exception report ○ store in line with data protection.
2.20	**Be able to escalate information about security incidents/events while preserving evidence** • Record details of incident/event: ○ the date and time of the incident/event ○ a description of the incident/event. • Take appropriate action: ○ isolate the device from the network if required. • Preserve the digital evidence: ○ take a copy of relevant digital log files. • Escalate the incident/event as appropriate.
2.21	**Understand, apply and monitor security controls according to NCSC Cyber Essentials** • Boundary firewalls and internet gateways – applied to restrict the flow of traffic in systems. • Secure configuration – applied to ensure users have only the required functionality (for example, removing unnecessary software, configuration to limit web access). • Malware protection – applied to maintain up-to-date anti-malware software and regular scanning. • Security update management – applied to maintain system and software updates to current levels.

	• Access control and management – applied when restricting access to a minimum, based on user attributes (for example, principle of least privilege, username and password management) – when special access is required above the standard user, then Privileged Access Management (PAM) would be implemented (for example, super user account, privileged business user).

2.22	**Understand the types and application of encryption tools as a risk mitigation technique**
	• Asymmetric encryption – applied to send private data from one user to another (for example, encrypted email systems):
	  ○ data in transit encryption:
	  – transport layer security (TLS) – applied to encrypt end-to-end communication in email, websites and instant messaging
	  – secure sockets layer (SSL) – a legacy protocol applied to create an encrypted link between a website and a browser using security keys for businesses to protect data on their websites.
	• Symmetric encryption – applied to encrypt and decrypt a message using the same key (for example, card payment systems):
	  ○ data at rest encryption (DARE):
	  – full disk encryption (FDE) – applied to encrypt the entire contents of a computer, used in situations to ensure that no data can be left unencrypted on a device (for example, this mitigates against theft of a laptop computer)
	  – file based encryption (FBE) – applied to encrypt individual files and folders, can be used when transferring sensitive documents between computers and individuals to prevent eavesdropping or tampering.

2.23	**Understand the purpose, criteria and types of back-ups utilised in risk mitigation**
	• Purpose:
	  ○ to maintain an up-to-date copy of data to enable future recovery and restoration for full disaster recovery or partial data loss.
	• Criteria:
	  ○ frequency – a schedule signalling the required periodic back-up (for example, daily, weekly, monthly)
	  ○ source – the information that is being backed up (for example, files or data)
	  ○ destination – the internal or external location of the information
	  ○ storage – the information must be stored safely in an appropriate format (for example, magnetic tape, disk) and location (for example, onsite, cloud, secondary site) ready for restoration as required
	  ○ retention – the length of time the backed-up data is retained
	  ○ test – the testing of restore files on a regular basis to ensure that a back-up will be ready in the event of a disaster.

	• Types:
	  ○ full – the creation of at least one additional copy of information
	  ○ incremental – a back-up of only the information that has changed since the previous full or incremental backup
	  ○ differential – a back-up of files that have changed since the last full backup
	  ○ mirror – a back-up of the information at a given time
	  ○ immutable – a back-up that cannot be changed, overwritten or deleted.

2.24	**Understand the purpose of organisational digital use policies and procedures to support risk mitigation** • Data protection policy – standardises the use, monitoring and management of data. • Acceptable use policy – provides information on the way in which networks or infrastructure should be used. • Access control policy – provides information on how access and permissions of users is managed. • Asset classification policy – influences the amount and complexity of controls that are applied to protect the asset, access controls, disposal and recovery objectives. • Information security policy – outlines requirements to use networks and infrastructure in a secure way. • Incident response procedure – outlines how an organisation will respond to an incident/event. • Mobile device policy – details standards, procedures and restrictions for users, connecting mobile devices to organisational infrastructure. • Back-up policy – details standards and procedures for performing backups to prevent loss of data. • Bring your own device (BYOD) policy – details requirements and restrictions when undertaking work activities using personally owned devices. • Password policy – provides information on computer security by requiring users to utilise strong passwords. • Asset disposal policy – provides guidance on the secure disposal of hardware when no longer in use. • Data retention policy – determines how long certain types of data must be kept.
2.25	**Be able to utilise a compliance and monitoring plan to monitor cyber security compliance** • Audit processes and policies to ensure they remain up to date (for example, review of information security policy): ○ improve and maintain processes and policies as required. • Compare and check accuracy of processes, log files and incident/ event reports. • Comply with ISO standards.

Content area 3: Discover, evaluate and apply reliable sources of knowledge

What underpinning knowledge do students need?	

3.1	**Understand and be able to identify a range of potential sources of knowledge applicable to cyber security**
	• Academic publications (for example, textbooks, research journals and periodicals).
	• Supplier literature (for example, Microsoft, Amazon Web Services).
	• Websites (for example, wikis, forums, community encyclopaedias, manufacturers' websites, question and answer websites).
	• Webinars (for example, information sharing by industry professionals).
	• Social media (for example, company profiles for Twitter/X, Facebook and LinkedIn).
	• Blogs (for example, discussions around vulnerabilities).
	• Vlogs (for example, tutorials on cyber security mitigation strategies).
	• Professional networks (for example, cyber security networking events/conferences).
	• Professional bodies (for example, Chartered Institute of Information Security (CIISec), Council of Registered Ethical Security Testers (CREST), Information Systems Audit and Control Association (ISACA), UK Cyber Security Council).
	• E-learning (for example, massive open online courses (MOOCs)).
	• Peers (for example, colleagues, network contacts, other industry professionals).
	• Cyber security policies and procedures (for example, information security policy).
	• Guidelines and legislation (for example, Data Protection Act 2018).
	• Regulating authorities (for example, ICO).
	• Industry standards (for example, NCSC Cyber Essentials, Centre for Internet Security (CIS) Benchmarks).
	• Industry accreditation (for example, CompTIA, Certified Cyber Professional (CCP), International Information System Security Certification Consortium (ISC)).
	• Databases (for example, CVE).
	• Be able to identify 3 sources of knowledge:
	  ○ identify the purpose and parameters of the topic or scenario
	  ○ identify 3 appropriate sources of knowledge to support the topic or scenario (for example, websites, community encyclopaedias, question and answer websites).
	(M5, D3, D5)

3.2	**Understand the factors of reliability and validity to be applied to legitimise the use of sources of knowledge and information**
	• Credibility of publisher (for example, author, organisation):
	  ○ affiliated to specific bodies (for example, government, industry regulators)
	  ○ reputation
	  ○ experience (for example, relevant qualification in subject)
	  ○ industry-certified accreditation.
	• Supported by credible citations.
	• Knowledge and information are relevant to the context.
	• Currency of the publication:
	  ○ version number (for example, use of the current version)
	  ○ date of publication (for example, is the content outdated?).
	• Absence of bias – personal opinions have not influenced source or information.
	• Recommend and justify actions to ensure the most reliable and valid information is utilised (for example, which information may or may not be valid and reliable and why, whether there is a requirement to find additional information).

3.3	**Be able to search for information from sources to support a topic or scenario** • Identify requirements of topic or scenario. • Search sources and extract relevant information (for example, information on threat intelligence, common attack techniques, cyber security policies and procedures, relevant guidelines, legislation and standards, evolving cyber security issues). (M5, D1, D6)
3.4	**Understand the factors affecting bias and be able to identify bias when using sources of knowledge in a specific cyber security context** • Author/propriety bias – unweighted opinions of the author or owner. • Confirmation bias – an individual may search for, interpret, favour and recall information that reinforces or confirms their prior beliefs or values. • Selection bias – refers to the inclination to select individuals, groups or data in a way that randomisation is not achieved. • Cultural bias – implicit assumptions based on societal norms. • Availability bias – an individual's opinion based on most recent or vivid experiences or memories.

	• Identify bias:
	  ○ identify the types of bias (for example, confirmation, unconscious)
	  ○ identify the indicators of bias within the source
	  ○ explain clearly and concisely how bias has been created within the source
	  ○ explain clearly and concisely how bias can be avoided within sources.

3.5	**Understand the application of potential evaluation techniques and tools**
	• Evaluation techniques:
	  ○ triangulation – validation of data or information by cross-checking from more than two sources to check the consistency of the results from different sources
	  ○ formative evaluation – an evaluation that takes place before or during the implementation of a task to make improvements
	  ○ summative evaluation – an evaluation that takes place at the end of a task to review achievements and inform future actions
	  ○ observation – reviewing and monitoring of a task in real time
	  ○ corroboration – the strengthening of existing information by cross-referencing information from other sources
	  ○ conclusions – a summary of the accuracy or appropriateness of the results
	  ○ recommendations – suggestions for future actions and decisions (for example, information security training).
	• Evaluation tools:
	  ○ gap analysis – to assess the current situation of existing control measures compared to a desired situation
	  ○ maturity assessments – to measure an organisation's ability to meet predictable outcomes
	  ○ user diaries – to provide a timely and accurate documentation of an ongoing process.

3.6	**Understand and be able to demonstrate the key stages of critical thinking to support objective evaluation**
	• Identification of relevant information:
	  ○ different arguments, views and opinions.
	• Analysis of identified information:
	  ○ considering bias and objectivity
	  ○ establishing links between information and data.
	• Selection of relevant evaluation techniques and tools.
	• Evaluation of findings.
	• Drawing conclusions.

	• Apply the process of critical thinking to meet requirements: o identify relevant information o analyse the information o select and apply appropriate evaluation techniques and tools o evaluate findings o logically organise and record conclusions. • Select and apply techniques and tools to support evaluation in a digital infrastructure context: o identify and clarify the parameters of the evaluation o select appropriate techniques and tools to support the evaluation o apply the selected techniques and use the appropriate tools to support the evaluation o record the findings of the evaluation for the requirement. (E1, E3, E4, E6, M1, M2, M3, M8, M10, D4)
3.7	**Understand types and purpose of potential communication methods used to share cyber security information and knowledge** • Digital services – digitally based technology that supports communication and enables 2-way communication: o helpdesk o phone o emails o SMS o chat messages. • Social media channels – supports conversations, community, connecting with an audience and building relationships: o organisational o public o community o personal. • Knowledge bases and knowledge management systems – a repository of information produced by one or more authors: o wikis o cyber security body of knowledge (CyBOK) o MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) o blogs o information security training platform o industry/vendor subscriptions or updates. • Project management tools – to communicate, track and visualise key information and progress throughout a task or project: o issue logs o Gantt charts o Kanban boards o burndown charts.

3.8	**Understand the potential impacts of cyber security issues on critical national infrastructure**
	• Supply chain:
	  ○ disruption to the supply of food and raw materials.
	• Utilities:
	  ○ energy sources:
	  – power cuts
	  – surges
	  – under-voltage events
	  – restricted or loss of gas supply
	  ○ water and sanitation:
	  – loss of fresh water to homes
	  – flooding
	  – disruption to water treatment/facilities
	  ○ government:
	  – interruptions to national communication channels
	  – interruptions to implementation of policies
	  ○ finance:
	  – failure of scheduled payments
	  – interruption to electronic transfers
	  – inability to process physical payments
	  ○ healthcare:
	  – compromised confidentiality, loss or damage to patient records
	  – impact on communications and ability to treat patients
	  ○ communication technologies and internet service providers:
	  – loss of service
	  – interruptions to businesses and individuals
	  – eavesdropping
	  – impersonation
	  ○ defence:
	  – impact on country's military and defence capabilities
	  ○ transport:
	  – disruption to privately or publicly owned modes of transport (for example, buses, trains, airlines)
	  – emergency services dispatch:
	  ▪ disruption to response times and capabilities.

3.9	**Understand the purpose and types of control systems**
	• Purpose:
	  ○ to receive data from remote sensors
	  ○ to measure values
	  ○ to control a process or an asset, where required, across different locations.

	• Types:
	  ○ industrial control systems – supports critical national infrastructure
	  ○ medical control systems – supports control of life-sustaining equipment and patient data
	  ○ facility-related control systems – supports control of securing facilities (for example, door locks)
	  ○ automotive control systems – controls everything in a vehicle (for example, engine and fuel systems).

3.10	**Understand the evolving cyber security risks associated with Internet of Things (IoT) devices**
	• Poor data protection controls:
	  ○ devices often have insufficient security controls built in to protect them from threats
	  ○ devices are usually too low-powered to support encryption and often give access to shared networks.
	• Poor password protection:
	  ○ weak or predictable passwords (for example, use of factory setting password).
	• Insecure data transfer and storage:
	  ○ during processing, transit or at rest, sensitive data is not encrypted or controlled by the system.
	• Security updates:
	  ○ lack of ability to securely update the device; as a result, firmware is not validated on devices, secure delivery is not secured, anti-rollback mechanisms are not in place and security updates are not notified of security changes.

3.11	**Understand the importance of information assurance and governance (IAG)** • Guides the development and improvement of IAG strategies, policies and processes. • Supports the auditing of current IAG strategies, policies and processes. • Informs the maintenance of IAG strategies, policies and processes through compliance monitoring plan. • Provides confirmation of compliance (for example, with ISO standards, NIST cyber framework).

3.12	**Be able to compare sources and recommend actions to ensure reliability and validity of sources**
	• Compare sources by applying the factors of reliability and validity:
	  ○ credibility of publisher (for example, author, organisation)
	  ○ currency of publication.
	• Recommend and justify actions to ensure the most reliable and valid source is utilised (for example, which sources may or may not be valid and reliable and why, whether there is a requirement to find additional sources).
	(M5, M6, D5)

Scheme of Assessment

There is a single synoptic assessment for this Occupational Specialism, which is an extended project. The synoptic element of the project is important to ensure students can demonstrate threshold competence and are able to evidence all the skills required by the Performance Outcomes.

The project consists of several activities grouped into four substantive tasks.

Each task is completed during a window set by Pearson, during which Providers schedule supervised assessment sessions. In some cases, tasks also include opportunities for unsupervised activities, where the requirements of the skills being assessed make this necessary.

Occupational Specialism project – Digital Infrastructure
Internally assessed project: 37 hours 30 minutes **99 marks**
Performance Outcomes In this project students will: **PO1** – Apply procedures and controls to maintain the digital security of an organisation and its data **PO2** – Explain, install, configure, test and manage both physical and virtual infrastructure **PO3** – Discover, evaluate and apply reliable sources of knowledge
Assessment overview There are three parts to the assessment: • Task 1: Analysing a problem and designing a solution • Task 2: Developing the solution • Task 3: Evaluating the system. Students respond to a given scenario to complete a substantial project. They are assessed on their application of the skills listed for the Performance Outcomes. Students are not assessed against specific 'knowledge' outcomes but are expected to draw on and apply related knowledge to ensure appropriate outcomes when applying the skills in response to an assessment scenario. Students undertake the project under a combination of supervised and controlled conditions. Internet access is permitted for all tasks except Task 3. The assessment takes place over multiple sessions, up to a combined duration of 37.5 supervised hours. The project outcomes consist of a portfolio of evidence submitted electronically. This project is externally marked by Pearson.

Occupational Specialism project – Digital Infrastructure
Administration Providers must follow the guidance in the following: • General Administrative Support Guide • Administration Support Guide for the specific Technical Qualification Occupational Specialism Project (if applicable) These are located on the Training and Admin Support webpage.

Occupational Specialism project – Network Cabling
Internally assessed project: 37 hours 30 minutes **111 marks**
Performance Outcomes In this project students will: **PO1** – Apply procedures and controls to maintain the digital security of an organisation and its data **PO2** – Install and test cabling in line with technical and security requirements **PO3** – Discover, evaluate and apply reliable sources of knowledge
Assessment overview There are three parts to the assessment: • Task 1: Analysing a problem and designing a solution • Task 2: Developing the solution • Task 3: Evaluating the network cabling solution. Students respond to a given scenario to complete a substantial project. They are assessed on their application of the skills listed for the Performance Outcomes. Students are not assessed against specific 'knowledge' outcomes but are expected to draw on and apply related knowledge to ensure appropriate outcomes when applying the skills in response to an assessment scenario. Students undertake the project under a combination of supervised and controlled conditions. Internet access is permitted for all tasks except Task 3. The assessment takes place over multiple sessions, up to a combined duration of 37.5 supervised hours. The project outcomes consist of a portfolio of evidence submitted electronically. This project is externally marked by Pearson.
Administration Providers must follow the guidance in the following: • General Administrative Support Guide • Administration Support Guide for the specific Technical Qualification Occupational Specialism Project (if applicable) These are located on the Training and Admin Support webpage.

Occupational Specialism project – Digital Support
Internally assessed project: 37 hours 30 minutes **99 marks**
Performance Outcomes In this project students will: **PO1** – Apply procedures and controls to maintain the digital security of an organisation and its data **PO2** – Install, configure and support software applications and operating systems **PO3** – Discover, evaluate and apply reliable sources of knowledge
Assessment overview There are three parts to the assessment: • Task 1: Analysing a problem and designing a solution • Task 2: Developing the solution • Task 3: Evaluating the support solutions. Students respond to a given scenario to complete a substantial project. They are assessed on their application of the skills listed for the Performance Outcomes. Students are not assessed against specific 'knowledge' outcomes but are expected to draw on and apply related knowledge to ensure appropriate outcomes when applying the skills in response to an assessment scenario. Students undertake the project under a combination of supervised and controlled conditions. Internet access is permitted for all tasks except Task 3. The assessment takes place over multiple sessions, up to a combined duration of 37.5 supervised hours. The project outcomes consist of a portfolio of evidence submitted electronically. This project is externally marked by Pearson.
Administration Providers must follow the guidance in the following: • General Administrative Support Guide • Administration Support Guide for the specific Technical Qualification Occupational Specialism Project (if applicable) These are located on the Training and Admin Support webpage.

Occupational Specialism project – Cyber Security
Internally assessed project: 37 hours 30 minutes **99 marks**
Performance Outcomes In this project students will: **PO1** – Apply procedures and controls to maintain the digital security of an organisation and its data **PO2** – Propose remediation advice for a security risk assessment **PO3** – Discover, evaluate and apply reliable sources of knowledge
Assessment overview There are four parts to the assessment: • Task 1: Analysing a problem and designing a solution • Task 2: Developing the solution • Task 3: Evaluating the system. Students respond to a given scenario to complete a substantial project. They are assessed on their application of the skills listed for the Performance Outcomes. Students are not assessed against specific 'knowledge' outcomes but are expected to draw on and apply related knowledge to ensure appropriate outcomes when applying the skills in response to an assessment scenario. Students undertake the project under a combination of supervised and controlled conditions. Internet access is permitted for all tasks except Task 3. The assessment takes place over multiple sessions, up to a combined duration of 37.5 supervised hours. The project outcomes consist of a portfolio of evidence submitted electronically. This project is externally marked by Pearson.
Administration Providers must follow the guidance in the following: • General Administrative Support Guide • Administration Support Guide for the specific Technical Qualification Occupational Specialism Project (if applicable) These are located on the Training and Admin Support webpage.

Performance Outcome (Digital infrastructure)		Weighting	
		Raw marks	% of total marks
PO1	Apply procedures and controls to maintain the digital security of an organisation and its data	45	45.5%
PO2	Explain, install, configure, test and manage both physical and virtual infrastructure	34	34.3%
PO3	Discover, evaluate and apply reliable sources of knowledge	20	20.2%

Performance Outcome (Network cabling)		Weighting	
		Raw marks	% of total marks
PO1	Apply procedures and controls to maintain the digital security of an organisation and its data	29	26.1%
PO2	Install and test cabling in line with technical and security requirements	56	50.5%
PO3	Discover, evaluate and apply reliable sources of knowledge	26	23.4%

Performance Outcome (Digital support)		Weighting	
		Raw marks	% of total marks
PO1	Apply procedures and controls to maintain the digital security of an organisation and its data	39	39.4%
PO2	Install, configure and support software applications and operating systems	36	36.4%
PO3	Discover, evaluate and apply reliable sources of knowledge	24	24.2%

Performance Outcome (Cyber security)		Weighting	
		Raw marks	% of total marks
PO1	Apply procedures and controls to maintain the digital security of an organisation and its data	35	35.4%
PO2	Propose remediation advice for a security risk assessment	38	38.4%
PO3	Discover, evaluate and apply reliable sources of knowledge	26	26.3%

Resources for the delivery of Occupational Specialism: Digital Infrastructure

Providers are required to have the following resources to deliver this OS:

- access to up-to-date PC or MAC computers with a specification that meets (or exceeds) the recommended requirements to run Cisco Packet Tracer software, office productivity software and internet browser software
- access to hardware and software resources to perform installation and configuration tasks. Examples include standalone desktop computers and laptops. Alternatively, students can install and configure software in a virtualised environment, providing that they do not compromise the security or operation of other 'live' systems
- equipment to capture or generate media assets
- teachers with qualifications and/or experience in the digital sector
- a curriculum team with experience and knowledge that spans the breadth of the qualification content.

	Resource required
General	• Word processing and spreadsheet software (such as MS Office). • Internet access. • Printer.
Specific	• Network diagramming software including packet tracer or appropriate alternative that can read a .pkt file. • Hardware and software resources or a virtualised environment to perform network installation and configuration tasks, including: o operating systems o software for end user devices and servers o anti-virus software o firewall software o access to computers capable of virtualisation o desktop virtualisation software o USB drives/pens and/or external hard drives o access to WiFi.

Resources for the delivery of Occupational Specialism: Network Cabling

Providers are required to have the following resources to deliver this OS:

- access to up-to-date PC or MAC computers with a specification that meets (or exceeds) the recommended requirements to run Cisco Packet Tracer software, office productivity software and internet browser software
- access to hardware and software resources to perform installation and configuration tasks. Examples include standalone desktop computers and laptops. Alternatively, students can install and configure software in a virtualised environment, providing that they do not compromise the security or operation of other 'live' systems
- equipment to capture or generate media assets
- teachers with qualifications and/or experience in the digital sector
- a curriculum team with experience and knowledge that spans the breadth of the qualification content.

	Resource required
General	• Word processing and spreadsheet software (such as MS Office). • Internet access. • Printer.

Specific	• Network diagramming software including packet tracer or appropriate alternative that can read a .pkt file.
	• Hardware and software resources or a virtualised environment to perform network installation and configuration tasks, including:
	  ○ operating systems
	  ○ software for end user devices and servers
	  ○ anti-virus software
	  ○ firewall software
	  ○ access to computers capable of virtualisation
	  ○ desktop virtualisation software.
	• Network cabling hardware including:
	  ○ UTP cable
	  ○ RJ45 cable connectors
	  ○ wall sockets
	  ○ patch panel
	  ○ cable termination tools (for example wire cutters, crimping tools)
	  ○ cable testing tools (for example network cable tester, tone generator and probe)
	  ○ labelling machine
	  ○ network cabling fixtures and fitting such as trunking, cable ties etc.
	• Network switch.
	• Router.
	• WiFi access point.

Resources for the delivery of Occupational Specialism: Digital Support

Providers are required to have the following resources to deliver this OS:

- access to up-to-date PC or MAC computers with a specification that meets (or exceeds) the recommended requirements to run Cisco Packet Tracer software, office productivity software and internet browser software
- access to hardware and software resources to perform installation and configuration tasks. Examples include standalone desktop computers and laptops. Alternatively, students can install and configure software in a virtualised environment, providing that they do not compromise the security or operation of other 'live' systems
- equipment to capture or generate media assets
- teachers with qualifications and/or experience in the digital sector a curriculum team with experience and knowledge that spans the breadth of the qualification content.

	Resource required
General	• Word processing and spreadsheet software (such as MS Office). • Internet access. • Printer.
Specific	• Network diagramming software including packet tracer or appropriate alternative that can read a .pkt file. • Hardware and software resources or a virtualised environment to perform network installation and configuration tasks, including: o operating systems o software for end user devices and servers o access to computers capable of virtualisation o desktop virtualisation software o USB drives/pens and/or external hard drives o access to WiFi. o mobile device (tablet or smartphone) o anti-virus software o PDF reader software o alternative web browser o email client software o intranet software.

Resources for the delivery of Occupational Specialism: Cyber Security

Providers are required to have the following resources to deliver this OS:

- access to up-to-date PC or MAC computers with a specification that meets (or exceeds) the recommended requirements to run Cisco Packet Tracer software, office productivity software and internet browser software
- access to hardware and software resources to perform security installation and configuration tasks. Examples include standalone desktop computers and laptops. Alternatively, students can install and configure software in a virtualised environment, providing that they do not compromise the security or operation of other 'live' systems
- equipment to capture or generate media assets
- teachers with qualifications and/or experience in the digital sector
- a curriculum team with experience and knowledge that span the breadth of the qualification content.

	Resource required
General	• Word processing software (such as MS Word) to generate written evidence/reports. • Internet access.
Specific	• Network diagramming software including packet tracer or appropriate alternative that can read a .pkt file • Hardware and software resources or a virtualised environment to perform security installation and configuration tasks, including: o operating systems o software for end user devices and servers o anti-virus software o anti-malware software o vulnerability scanning software o firewall software o access to computers capable of virtualisation o desktop virtualisation software o USB drives/pens o access to WiFi.

5 Technical Qualification grading, T Level grading and results transfer

How the Technical Qualification is graded and awarded

Calculation of the Technical Qualification grade

The Technical Qualification components are awarded at the grade ranges below.

Component	Available grade range
Core (including Core examination/s and Employer Set Project)	A* – E and Unclassified
Occupational Specialism	Distinction, Merit, Pass and Unclassified

The Core uses an aggregation of points from each of the Core assessments to calculate the A* to E grade.

Students whose level of achievement for either component is below the minimum judged by Pearson to be of sufficient standard receive an Unclassified (U) result.

Awarding the components

Grade boundaries will be set for each component and/or sub-component (Core Examinations, Employer Set Project and Occupational Specialism) in each series they are offered through a process known as awarding. Awarding is used to set grade boundaries and ensure standards are maintained over time. This is important as we must ensure students have the same opportunity to achieve, regardless of the assessment opportunity.

Uniform Mark Scale

For the Core component, students' raw component and/or sub-component marks are converted to a Uniform Mark Scale (UMS). The UMS is used to convert students' 'raw' marks into uniform marks. This is done to benchmark outcomes from one series to another to account for any variety of difficulty in assessments. For example, a student who produces a response worthy of a C grade in the Employer Set Project in one series will receive the same uniform mark as a student achieving that same grade and level of performance in another series, regardless of their raw marks.

The maximum number of uniform marks available for each sub-component, and the uniform marks relating to each grade boundary, are fixed. These are shown below.

Grade	Core Exam	Core ESP	Core Overall
Maximum	**240**	**160**	**400**
A*	216 – 240	144 – 160	360 – 400
A	192 – 215	128 – 143	320 – 359
B	168 – 191	112 – 127	280 – 319
C	144 – 167	96 – 111	240 – 279
D	120 – 143	80 – 95	200 – 239
E	96 – 119	64 – 79	160 – 199
U	0 – 95	0 – 63	0 – 159

Where the Core component has two Core Exams, the results are combined before conversion to UMS.

Calculation of the T Level grade

The T Level grade look-up table shows the minimum thresholds the Department for Education use for calculating the T Level grade.

Students must complete both components and achieve a minimum of a grade E in the Core and a Pass in the Occupational Specialism. In addition, they must successfully complete the other elements of the T Level, such as the industry placement.

Students who do not meet the minimum requirements will not be certificated.

Results transfer to Providers

Technical Qualification result days:

Assessment series	Results day
Summer	August (Level 3 Results Day)
November	March (normally the third week − Level 3 Results Day)

Pearson issues the results directly to you and makes available:

- Scorecards: outlining the achievement in percentage terms against each Assessment Objective
- Results Plus: a service whereby achievement will be presented in an item-by-item format. This means Providers will be able to ascertain trends across and within cohorts, and clearly label the associated Assessment Objective
- Statement of Provisional Results: we will offer a provisional component result slip, clearly watermarked as a provisional component result.

As we are not required to issue Technical Qualification certificates, T Level certificates or T Level statements of achievement, we do not require you to complete any forms or processes to claim the Technical Qualification from Pearson.

T Level Results reporting

The Technical Qualification forms part of the T Level.

The Department for Education will issue T Level results on Level 3 results day in August.

The Department for Education will provide T Level certificates to students who successfully complete all elements of the T Level.

Appendix 1: General Competency Frameworks for T Levels

The General Competency Framework for T Levels articulates English, maths and digital competencies that students are required to develop over the course of the qualification. The tables below list the competencies from the framework that are relevant to the *T Level Technical Qualification in Digital Support and Security*.

Competencies that can be developed in relation to a specification element of content are referenced in the column next to this content element in the occupational specialism. These competencies should be delivered through the content of this qualification and teachers should seek opportunities to allow students to develop the relevant skills to enable them to reach threshold competence in the specialism.

The English, maths and digital competencies are embedded in both the Core Component and the Occupational Specialism Component of the *T Level Technical Qualification in Digital Support and Security*. This is so that students can demonstrate their knowledge and understanding of these skills over the course of the qualification.

General English competencies

Students should be supported to develop the English knowledge and skills needed in order to:

E1	Convey technical information to different audiences
E2	Present information and ideas
E3	Create texts for different purposes and audiences
E4	Summarise information/ideas
E5	Synthesise information
E6	Take part in/leading discussions

General maths competencies

Students should be supported to develop the maths knowledge and skills needed in order to:

M1	Measure with precision
M2	Estimate, calculate and spot errors
M3	Work with proportion
M4	Use rules and formulae
M5	Process data
M6	Understand data and risk
M7	Interpret and represent with mathematical diagrams
M8	Communicate using mathematics
M9	Cost a project
M10	Optimise work processes

General digital competencies

Students should be supported to develop the digital knowledge and skills needed in order to:

D1	Use digital technology and media effectively
D2	Design, create and edit documents and digital media
D3	Communicate and collaborate
D4	Process and analyse numerical data
D5	Be safe and responsible online
D6	Code and program

Command word taxonomy list

The following table shows the command words that will be used consistently in our assessments to ensure students are rewarded for demonstrating the necessary skills. The list below will not necessarily be used in every paper and is provided for guidance only.

Command word	Definition
Give/state/name	Provide a response (e.g. a feature, a characteristic, a use of or a justification for something).
Identify	Select the correct answer from the given context or stimulus.
Write	Write formula using information from the given context or stimulus.
Describe	Provide responses that are linked in an appropriate logical order.
Explain	Requires identification of a point and linked justification of that point.
Explain with additional justification	Requires identification of a point, a linked justification and a third point, which is a further justification of the first justification.
Discuss	Consider the factors that apply in relation to a specific context. Give careful consideration to opposing aspects of an issue, situation or problem. A conclusion is not required.
Evaluate	Consider various aspects of a subject's qualities in relation to its context, such as strengths and weaknesses, advantages and disadvantages, pros and cons. Come to a judgement supported by evidence which will often be in the form of a conclusion.
Draw	Produce a diagram (e.g. an algorithm, a process flow) using information from a given context or scenario.
Complete	Provide the missing information for a diagram so that it is complete (contains all the necessary information).

Appendix 2: Diagrams

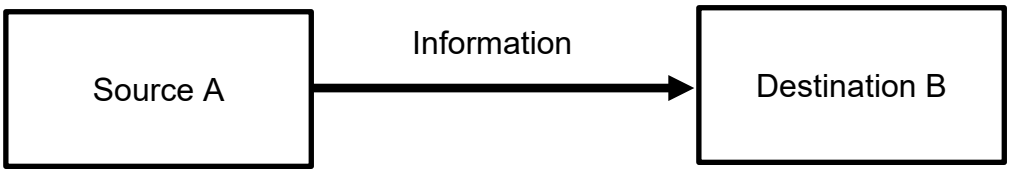
This appendix provides additional information about the digital technologies that students are expected to learn about within the core and occupational specialism content.

This appendix does not replace the specification but should be used alongside the specification content to provide additional guidance and scope.

Sections of the specification that do not require additional expansion are not included.

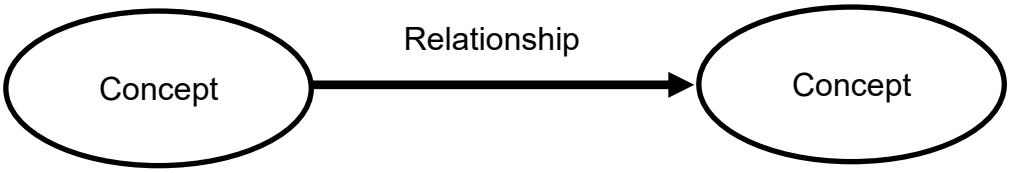
Information flow diagrams

Students should be able to use and create appropriately labelled diagrams to express meaning.



Concept map symbols

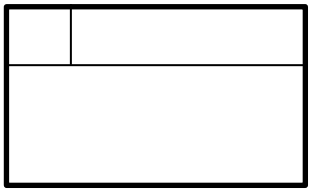
Relationship is expressed as a verb.



Data flow diagrams

Arrows and labels as required.

Denotes data source of destination (inputs and outputs)



Denotes a process

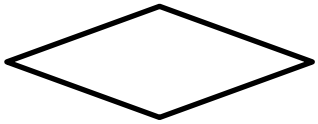
Denotes a data store

Flowchart symbols

Denotes the start and end of an algorithm

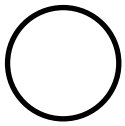
Denotes a process to be carried out

Denotes a sub-process



Denotes a decision to be made

Denotes input or output



Denotes a connection to part of a flow chart that cannot easily be linked using an unbroken flow arrow

Shows the logical flow of the program

Explore Pearson's T Levels offering at
https://qualifications.pearson.com/en/qualifications/t-levels.html