T-LEVELS | Institute for Apprenticeships & Technical Education

Qualification specification

T Level Technical Qualification in Digital Support Services

Version 1.5 March 2022 603/6901/2
Internal reference: TQ-Digital Support-spec

NCFE

T Level Technical Qualification in Digital Support Services Qualification Specification

Digital Support Services

603/6901/2

Contents

Section 1: Introduction

A T Level[1] is a composite technical study programme, aimed at preparing young people for work, higher level apprenticeships or higher education (HE). It comprises 5 key components:

- an approved technical qualification, which includes the opportunity to specialise in at least one occupational role
- a substantial industry placement with an external employer (further information regarding the required number of hours can be found on page 8)
- English, mathematics and digital requirements; students will have to achieve a minimum of level 2 English and mathematics in order to achieve a T Level (with some flexibility for students with special educational needs or disabilities (SEND))
- employability, enrichment and pastoral elements (EEP)
- in some cases, it may also include mandatory additional requirements (MAR), such as important licence to practise qualifications

The T Level Technical Qualification in Digital Support Services forms part of the new T Level in digital support services. The outline content has been produced by T Level panels based on the same standards as those used for apprenticeships. The outline content formed the basis of this qualification and has been further developed by NCFE.

This qualification has 2 components:

- core component:
  - route core
  - pathway core
- occupational specialism components:
  - Digital infrastructure
  - Network cabling
  - Digital support

The route core provides a variety of knowledge and skills relevant to the digital route as a whole. The pathway core provides a variety of knowledge and skills relevant to the occupational specialism components within the digital support services TQ. Some of the pathway core topics and ideas are broken down and contextualised in more detail within the occupational specialisms, allowing students to apply the knowledge and skills in their own specific specialism.

[1] T Level is a registered trademark of the Institute for Apprenticeships and Technical Education

Each occupational specialism component covers the knowledge, understanding, skills and behaviours required to achieve threshold competence in a chosen occupational specialism. Threshold competence refers to the level of competence deemed by employers as sufficient to secure employment in roles relevant to an occupational specialism. Achievement of threshold competence signals that a student is well-placed to develop full occupational competence, with further support and development, once in work.

English, mathematics and digital skills have also been embedded throughout the technical qualification (TQ) and must be taught when highlighted in the content.

About this TQ specification

To ensure that you are using the most up-to-date version of this TQ specification, please check the version number and date in the page footer against that of the TQ specification on the NCFE website.

If you advertise this qualification using a different or shortened name, you must ensure that students are aware that their results will state the full regulated qualification title.

Section 2: Summaries

Technical qualification summary

Qualification title

T Level Technical Qualification in Digital Support Services

Qualification number (QN)

603/6901/2

Aim reference

60369012

Qualification level

3

Guided learning hours (GLH) and total qualification time (TQT)

Digital infrastructure	GLH for delivery	GLH for assessment	Total GLH	TQT
Core component	584	16 hours 40 minutes	600 hours 40 minutes	647
Occupational specialism	575	24 hours 30 minutes	599 hours 30 minutes	657
Total			1200 hours 10 minutes	1304

Network cabling	GLH for delivery	GLH for assessment	Total GLH	TQT
Core component	584	16 hours 40 minutes	600 hours 40 minutes	647
Occupational specialism	569	31	600	657
Total			1200 hours 40 minutes	1304

Digital support	GLH for delivery	GLH for assessment	Total GLH	TQT
Core component	584	16 hours 40 minutes	600 hours 40 minutes	647
Occupational specialism	566	34	600	657

Total			1200 hours 40 minutes	1304

The GLH only include time for the technical qualification element of the T Level programme; they do not include time allocated for the additional components of the T Level programme.

Minimum age

T Level Technical qualification students must be a minimum of 16 years of age.

Qualification purpose

The purpose of the T Level Technical Qualification in Digital Support Services is to ensure students have the knowledge and skills needed to progress into skilled employment or higher level technical training relevant to the T Level.

Objectives

The objectives of this qualification are to equip students with:

- the core knowledge and skills relevant to digital support services
- up-to-date occupational knowledge and skills that have continued currency amongst employers and others
- the necessary English, mathematics and digital skills
- threshold competence that meets employer expectations and is as close to full occupational competence as possible
- opportunities to manage and improve their own performance

Industry placement experience

Industry placements are intended to provide students with the opportunity to develop the knowledge, skills and behaviours required for skilled employment in their chosen occupation and which are less easily attainable by completing a qualification alone.

As part of achieving the overall T Level programme, students are required to complete a minimum of 315 hours industry placement. It is the provider's responsibility to ensure the minimum number of hours is undertaken by the student.

There may be specific requirements for providers and employers to consider prior to the student commencing a work placement. Please see the industry placement guidance from the Institute for Apprenticeships and Technical Education.

There are specific requirements for providers and employers relating to the insurance of students in the workplace. Further information about insurance can be found at www.abi.org.uk or www.hse.gov.uk/youngpeople/index.htm.

Rules of combination

Students are required to complete:

- core component:

  - route core
  - pathway core
- one occupational specialism component:
  - Digital infrastructure
  - Network cabling
  - Digital support

Students **must not** complete more than **one** occupational specialism component.

Approved providers can select which occupational specialism component to deliver to their students.

Grading

Component	Grade
Core component	A* to E and U
Occupational specialism component	Distinction/merit/pass and ungraded

Assessment method

Core component:

- 2 written examinations
- employer-set project (ESP)

In order to achieve a grade for the core component, students must have results for both sub-components (the core (written) examination and the ESP).

The combined results from these sub-components will be aggregated to form the overall core component grade (A*–E and U).

If students fail to reach the minimum standard across all sub-components, they will receive a U grade. No overall grade will be issued for the core component until both sub-components have been attempted.

Occupational specialism component:

- synoptic assignments

The student is also required to successfully achieve a distinction/merit/pass grade in one of the occupational specialism components. If the student fails to reach the specified level of attainment, they will receive a U grade.

Progression including job roles (where applicable)

Students who achieve this qualification could progress to the following, depending on their chosen occupational specialism:

- employment:
    - digital support technician:
        - digital applications technician
        - digital service technician
    - infrastructure technician
    - IT solutions technician:
- hardware solutions
- software solutions
    - network cable installer
- higher education
- apprenticeship (progression onto lower level apprenticeships may also be possible in some circumstances, if the content is sufficiently different)

UCAS

The T Level study programme is eligible for UCAS points. Please check the UCAS website for more information.

Regulation information

This is a regulated qualification. The regulated number for this qualification will be completed following Ofqual accreditation.

Funding

This qualification is eligible for funding. For further guidance on funding, please contact the Education and Skills Funding Agency (ESFA).

English, mathematics and digital content

English, mathematics and digital content are embedded and contextualised within the core skills and occupational specialism qualification content. This content must be taught to all students and will be subject to assessment.

Entry guidance

This qualification is designed for post-16 students.

There are no specific prior skills/knowledge a student must have for this qualification. However, students would be expected to have a level 2 qualification or equivalent.

Providers are responsible for ensuring that this qualification is appropriate for the age and ability of students. Providers must make sure that students can fulfil the requirements of the core component and chosen occupational specialism and comply with the relevant literacy, numeracy, digital and health and safety aspects of this qualification.

Students registered on this qualification should not undertake another qualification at the same level with the same or a similar title, as duplication of learning may affect funding eligibility.

Transition programme

For those students who are not yet ready to start a T Level programme at 16, they will be able to study a new T Level Transition Programme. This is a new 16 to 19 study programme designed to give young people effective, tailored preparation specifically to help them progress onto and succeed in a T Level.

The T Level Transition Programme will be introduced through phased implementation, working initially with a small number of volunteer T Level schools, colleges and training companies, to explore different approaches to delivery and develop good practice in effectively preparing students for a T Level. More information on the T Level Transition Programme can be found on the government's website.

Students transferring between T Levels

It is expected that some students will switch between T Levels, particularly in the early weeks, as happens currently with many post-16 courses. Some providers may co-teach some T Level groups for some classes where these are within the same route and where much of the core content is the same. This may well result in students switching to a different T Level, as they discover more about the content, including the range of occupational specialisms.

Depending on the point at which a student switches, they may need some additional support to catch up on any other pathway-specific learning they have missed.

During year 1, providers should consider the degree of overlap between 2 T Levels, and the remaining time pre-assessment, to determine which transfers should be permitted. For funding purposes, it is important that students have made a decision about their T Level and occupational specialism by the end of the first year. However, once an assessment has been taken, switching may become more difficult. T Level core assessments will vary in terms of content coverage, duration, and method, and therefore attainment from one T Level cannot count towards another.

Achieving this qualification

To achieve this qualification, the student must successfully demonstrate their achievement of the core component and one occupational specialism component.

In order to achieve a grade for the core component, the student must attempt both the external examination (paper A and paper B) and ESP sub-components. The results from these will be aggregated to form the overall core component grade (A* to E and U). If students do not attempt one of the sub-components, an overall component grade will be withheld pending the attempt of both. If students fail to reach the minimum standard across sub-components after attempting both, they will receive a U grade for the component.

The student is required to successfully achieve a distinction/merit/pass grade in one of the occupational specialism components. If the student fails to reach the specified level of attainment, they will receive a U grade.

Retakes

Core component retakes

There is the opportunity for students to retake the core component assessments in order to improve their marks. This includes:

- written examinations
- ESP

The core component's written examination is made up of 2 parts. If the student wants to retake the written examination assessment, they must retake **both** papers, in the same series, as achievement on individual papers cannot be combined across different series.

There is no limit to the number of retakes a student can complete. However, any retake must be completed within 2 years after the completion of the student's T Level programme.

When determining each student's overall achievement for the core component, the highest achievement in each core component assessment (written examination and ESP) is used.

Occupational specialism component retakes

Although retakes are permitted for the occupational specialism, it is unlikely that students will be able to fit a retake opportunity into the delivery timetable.

If a retake opportunity is scheduled, the student must retake all synoptic assignments for the chosen occupational specialism. There will be one opportunity per year to sit the occupational specialism, meaning a retake of the occupational specialism would be sat in the next academic year of study.

There is no limit to the number of retakes a student can complete. However, any retake must be completed within 2 years after the completion of the student's T Level programme.

Technical qualification components

Component	Level	Content
Route core component	3	R1. Business context R2. Culture R3. Data R4. Digital analysis R5. Digital environments R6. Diversity and inclusion R7. Learning R8. Legislation R9. Planning R10. Security R11. Testing R12. Tools
Pathway core component	3	P1. Careers within the digital support services sector P2. Communication in digital support services P3. Fault analysis and problem resolution

Students are required to complete one occupational specialism component.

Component	Level	Content
Digital infrastructure	3	• Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data • Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure • Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge
Network cabling	3	• Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data • Performance outcome 2: Install and test cabling in line with technical and security requirements

		• Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge
Digital support	3	• Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data • Performance outcome 2: Install, configure and support software applications and operating systems • Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Employer involvement

The outline content for this qualification was devised by T Level panels. The panels consisted of employers and industry stakeholders.

We have worked in partnership with employers and other stakeholders to elaborate the content further, create the assessments and set the standards to ensure students achieve the level of competence needed to enter skilled employment.

Progression to higher level studies

This qualification aims to provide students with a number of progression options, including higher level studies at university or further education (FE) colleges. The skills required to progress to higher academic studies are different from those required at levels 1 and 2. Level 3 qualifications enable the development of these skills. Although there is no single definition of higher level learning skills, they include:

- checking and testing information
- supporting points with evidence
- self-directed study
- self-motivation
- thinking for yourself
- analysing and synthesising information/materials
- critical thinking and problem solving
- working collaboratively
- reflecting upon learning and identifying improvements
- presenting information in written and verbal formats

Level 3 criteria can require students to analyse, draw conclusions, interpret or justify, which are all examples of higher level skills and support progression and further learning. If you need any further information, please refer to the NCFE website.

How the qualification is assessed

Assessment is the process of measuring a student's skill, knowledge and understanding against the standards set in a qualification.

The core component (route core and pathway core) is 100% externally assessed. External assessments are set and marked by NCFE. The external examinations and ESP will assess students' core knowledge, understanding and skills relevant to the occupations within the digital support services TQ. Students may be entered for any assessment window of the core component assessments that is most appropriate for them, although, in the case of the core external examinations, they must take the 2 examinations in the same sitting and, in their first attempt, students must take all the core assessments in the same assessment window.

The occupational specialism components are also externally assessed through synoptic assignments. These synoptic assignments will assess the knowledge, understanding, skills and behaviours required to achieve threshold competence in the student's chosen occupational specialism.

Providers must not give any feedback to the student about their performance in any of the externally assessed components or elements.

The assessment consists of:

- core component:
    - 2 written examinations
    - ESP
- occupational specialism component:
    - synoptic assignments (specific to each occupational specialism)

Assessment of English, maths and digital

The TQ outline content has been reviewed against the general competency frameworks for English, mathematics and digital (EMD). The resulting mapping document is contained in section 3.

For the purposes of the core tests, English skills will be assessed through the students' ability to convey ideas precisely and accurately and be referred to as quality of written communication (QWC).

Quality of written communication (QWC)

Quality of written communication is assessed within targeted marks for the core examinations and are embedded throughout the assessment objectives within the ESP. No specific marks are available within the occupational specialism; however, a good command of communication and written work is anticipated for success at this level.

Application of mathematics, significant figures and decimal places

Throughout the core component examinations for all pathways, students will be assessed on their understanding and application of mathematics. Some questions may require answers to be given to a number of significant figures or a given number of decimal places.

A paper may contain marks that are dependent on students giving final answers to a specified number of significant figures or decimal places. A significant figure mark may not be awarded for an answer given in surd form. In questions where the command word is 'calculate' and the final answer is required in either format, the question

should be calculated to at least one additional significant figure or decimal place before giving the final answer as requested in the question.

In all cases where an answer is required to a number of significant figures or decimal places, this will be specified in the question.

Digital skills

Digital skills are expected to be naturally occurring in the ESP and occupational specialism; marks are allocated where they are deemed to occur naturally in the completion of the task.

Rationale for synoptic assessment

Synoptic assessments test students' understanding of the connections between the topics covered across the performance outcomes within the chosen occupational specialism.

Synoptic assessment enables students to integrate and apply knowledge, understanding and skills with breadth and depth. It also requires them to demonstrate their capability to apply knowledge, understanding and skills across the chosen occupational specialism.

Scheme of assessment for each component

Each component in the core is worth the following weighting:

	% weighting of the core component
Paper A	34
Paper B	41
Sub-total	75
ESP	25
Total	**100%**

External examinations (core component)

Overview of assessment

Paper A
Written examination

Duration: 2 hours

100 Marks (plus 6 marks for quality of written communication) = 106 marks total

This paper covers 50% of the core knowledge and understanding

This paper is composed of 3 sections:

- Section A: Business context (element 1) and Culture (element 2): multiple choice questions, short-answer and extended writing, 38-44 marks

- Section B: Diversity and inclusion (element 6) and Digital environments (element 5): multiple choice questions, short-answer and extended writing, 36-42 marks
- Section C: Learning (element 7) and Planning (element 9): multiple choice questions, short-answer and extended writing, 20-26 marks

Paper B
Written examination

Duration: 2 hours 30 minutes

125 Marks (plus 6 marks for quality of written communication) = 131 marks total

This paper covers 50% of the core knowledge and understanding

This paper is composed of 4 sections:

- Section A: Digital Support Services pathway: multiple choice questions, short-answer and extended writing, 25 marks
- Section B: Tools (element 12) and Testing (element 11): multiple choice questions, short-answer and extended writing, 18-24 marks
- Section C: Security (element 10) and Legislation (element 8): multiple choice questions, short-answer and extended writing, 34-40 marks
- Section D: Data (element 3) and Digital analysis (element 4): multiple choice questions, short-answer and extended writing, 40-46 marks

Content subject to assessment

- Paper A:
    - route core elements: 1, 2, 5, 6, 7 and 9
- Paper B:
    - route core elements: 3, 4, 8, 10, 11 and 12
    - pathway core element: 1, 2 and 3

Assessment objectives and weightings

The external (core component) examinations will assess how students have achieved the following assessment objectives (AOs).

	Assessment objectives	**Weighting***
AO1	Demonstrate knowledge and understanding of the digital support services sector	28%
AO2	Apply knowledge and understanding of the digital support services sector to different situations and contexts	40%
AO3	Analyse and evaluate information and issues related to the digital support services sector	32%

*Both paper A and paper B allocate 6 marks to the Quality of Written Communication (QWC). These marks are bolted on and do not impact on the AO weightings. For example, paper A totals 106 marks of which the AO weightings apply to a total of 100 marks, with the remaining 6 assessing QWC.

Total marks

AOs	Paper A	Paper B	Total
AO1	28 marks (14%)	35 marks (14%)	63 marks (28%)
AO2	40 marks (20%)	50 marks (20%)	90 marks (40%)
AO3	32 marks (16%)	40 marks (16%)	72 marks (32%)
QWC	6 marks	6 marks	12 marks
Total	**106 marks**	**131 marks**	**237 marks**

The table above shows how the core examination will target the AOs in this qualification. Each version of the core examination will adhere to these mark and percentage weighting. Both paper A and paper B allocate 6 marks to the Quality of Written Communication (QWC). These marks are bolted on and do not impact on the AO weightings.

Assessment availability

There will be 2 assessment opportunities per year in Summer (May/June) and Autumn (November/December). Please refer to the Assessment timetable on the NCFE website for further information.

Assessment conditions

The core component external examinations must be invigilated.

All students' scripts must be submitted to NCFE for marking. All assessment material must be securely stored by the approved provider. On-screen assessments will be submitted through the online assessment platform.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Employer-set project (core component)

Overview of assessment

Externally-set (in conjunction with employers) project

The purpose of the employer-set project is to ensure that students have the opportunity to apply core knowledge and skills to develop a substantial piece of work in response to an employer-set brief. The brief and tasks are contextualised around an occupational area and chosen by the student ahead of the assessment window.

To achieve the AOs and meet the brief, the student must demonstrate the following core skills:

Core skill 1	Communicate information clearly to a technical and non-technical audience
Core skill 2	Work with stakeholders to clarify and consider options to meet requirements
Core skill 3	Apply a logical approach to solving problems, identifying and resolving faults whilst recording progress and solutions
Core skill 4	Ensure activity avoids risks to security

The knowledge requirements will be taken from the core knowledge relevant to the brief; the briefs will change for each assessment window.

Duration: 12 hours 10 minutes

Subject content to be assessed

Content subject to assessment – route core elements: 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12:

- core skills assessment objectives and core knowledge

Pathway core elements: 1, 2, 3

Core knowledge relevant to the brief will be covered in the employer-set project; this will change for each assessment window.

Core skills

In completing the employer-set project, the student will demonstrate 4 core skills, supported by underpinning knowledge and understanding set out in the core content.

Core skill 1	Communicate information clearly to a technical and non-technical audience
Core skill 2	Work with stakeholders to clarify and consider options to meet requirements
Core skill 3	Apply a logical approach to solving problems, identifying and resolving faults whilst recording progress and solutions
Core skill 4	Ensure activity avoids risks to security

Assessment objective (AO)		AO weighting
AO1	Plan their approach to meeting the project brief	16 marks (21)%
AO2	Apply core knowledge and skills as appropriate to infrastructure support and maintenance	40 marks (52.5)%
AO3	Select relevant techniques and resources to meet the brief	6 marks (8)%
AO4	Use English, mathematics and digital skills as appropriate	6 marks (8)%
AO5	Realise a project outcome and review how well the outcome meets the brief	8 marks (10.5)%

Task	AO1	AO2	AO3	AO4 (Maths)	AO4 (English)	AO5	TOTAL
1		16	6				22
2	8	4			4*		12*
3	8	16		2			26*
4		4				8	12*
Total marks	16	40	6	6		8	76* (when the x4 AO4 English are included)

*AO4 (English) is assessed holistically across tasks 2, 3 and 4 using two level of response mark schemes and is not included in the individual task totals - only the overall ESP total.

Assessment availability

There will be 2 assessment opportunities per year in Summer (May/June) and Autumn (November/December). Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under supervised conditions. This means students can access resources in order to complete their assessment.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

UMS

The core component is modular, which means that a student can take and resit the assessments in different assessment windows. Assessments may vary slightly in levels of difficulty and, therefore, the mark that represented a C grade in the external examination in one assessment window may not be appropriate in the following assessment window.

To address this, we convert raw marks to uniform marks. The UMS also allows us to account for the relative weighting of the assessment to the qualification as a whole. The maximum UMS points available for each assessment, and the UMS points relating to each grade boundary, are fixed. These are shown in the following table:

Grade boundary	External examination	Employer-set project	Overall
Max	300	100	400
A*	270	90	360
A	240	80	320
B	210	70	280
C	180	60	240
D	150	50	200
E	120	40	160
U	0	0	0

The external examination comprises 2 papers, the results of which are combined before conversion to UMS. Combined grade boundaries for each series will be set by adding together the equivalent boundaries for each paper.

The raw mark grade boundaries are set after each assessment window. NCFE sets these boundaries judgementally, following both qualitative and quantitative analysis, and then converts them to UMS.

Although the raw mark grade boundaries in assessment window 1 and assessment window 2 are different, they have the same value in terms of UMS marks (for example 180 for a C and 210 for a B) when contributing to the

qualification as a whole. NCFE will publish the raw mark grade boundaries following the completion of each assessment window.

Synoptic assignments (Digital infrastructure)

Synoptic assignments comprise task-based assignments.

Duration: 24 hours 30 minutes

Consisting of:

- assignment 1: 13 hours
- assignment 2: 6 hours
- assignment 3: 5 hours 30 minutes

Content subject to assessment

All performance outcomes within a chosen occupational specialism are subject to assessment:

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Assessment weightings

Assignment	% weighting of the Occupational Specialism	Max raw mark	Scaling factor*	Maximum scaled mark
Assignment 1	35%	76	1.000	76.000
Assignment 2	35%	53	1.434	76.000
Assignment 3	30%	56	1.163	65.143
Total	100%	185 marks		*217*

Total marks 185

*Scaled marks for assignments are calculated by multiplying the raw assessment mark with the scaling factor. Scaled marks up to 3 decimal places are combined before being rounded to the nearest whole number. The same approach is used to determine overall combined grade boundaries from assignment grade boundaries.

Assessment availability

There will be one assessment opportunity per year from Summer 2023. Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under specified conditions. See the tutor guidance in the tutor guidance pack for more detail.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Synoptic assignments (Network cabling)

Synoptic assignments comprise task-based assignments.

Duration: 31 hours

Consisting of:

- assignment 1: 13 hours
- assignment 2: 12 hours 30 minutes
- assignment 3: 5 hours 30 minutes

Content subject to assessment

All performance outcomes within a chosen occupational specialism are subject to assessment:

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install and test cabling in line with technical and security requirements
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Assessment weightings

Assignment	% weighting of the Occupational Specialism	Max raw mark	Scaling factor*	Maximum scaled mark
Assignment 1	30%	60	1.017	61.000
Assignment 2	40%	44	1.848	81.333
Assignment 3	30%	61	1.000	61.000
Total	100%	165 marks		*203*

Total marks 165

*Scaled marks for assignments are calculated by multiplying the raw assessment mark with the scaling factor. Scaled marks up to 3 decimal places are combined before being rounded to the nearest whole number. The same approach is used to determine overall combined grade boundaries from assignment grade boundaries.

Assessment availability

There will be one assessment opportunity per year from Summer 2023. Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under specified conditions. See the tutor guidance in the tutor guidance pack for more detail.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Synoptic assignments (Digital support)

Synoptic assignments comprise task-based assignments.

Duration: 34 hours

Consisting of:

- assignment 1: 19 hours
- assignment 2: 5 hours
- assignment 3: 10 hours

Content subject to assessment

All performance outcomes within a chosen occupational specialism are subject to assessment:

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install, configure and support software applications and operating systems
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Assessment weightings

Assignment	% weighting of the Occupational Specialism	Max raw mark	Scaling factor*	Maximum scaled mark
Assignment 1	50%	76	1.000	76.000
Assignment 2	20%	30	1.013	30.400
Assignment 3	30%	27	1.689	45.600
Total	100%	133 marks		*152*

Total marks 133

*Scaled marks for assignments are calculated by multiplying the raw assessment mark with the scaling factor. Scaled marks up to 3 decimal places are combined before being rounded to the nearest whole number. The same approach is used to determine overall combined grade boundaries from assignment grade boundaries.

Assessment availability

There will be one assessment opportunity per year from Summer 2023. Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under specified conditions. See the tutor guidance in the tutor guidance pack for more detail.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Core written examinations

The core written examinations will be available as onscreen and as paper-based examinations. A different version of each examination will be available per mode.

The ESP and the occupational specialism assessments will be released and accessed by providers electronically. The submission of any assessment evidence from providers will also be digital and provided to NCFE electronically, unless otherwise specified.

For instructions on conducting external assessments (including information on malpractice/maladministration), please refer to our regulation for the conduct of external assessments and qualification specific instructions for delivery documents, which are available on the Policies & Documents page on the NCFE website.

Sample assessment materials

Sample assessment materials can be found on the qualification page on the NCFE website.

Results

Results for each component will be released in accordance with the assessment windows. Please refer to the assessment windows on the NCFE website for further information.

Enquiries about results

If a provider believes a student's result is at variance with their reasonable expectations, they can submit an enquiry about a result in line with our enquiries about results and assessment decisions policy, which is available on the Policies & Documents page on the NCFE website.

Grading

Core component

The core component is graded A* to E and U.

Core component grade descriptors

Grade	Demonstration of attainment
A	The student will be able to:
	demonstrate **relevant** and **accurate** use of terminology
	demonstrate a **comprehensive** understanding of ideas, processes and procedures applied to familiar and unfamiliar contexts
	use a **range** of mathematical skills relevant to the sector
	critically analyse **most** information and data, supported with relevant examples and analysis
	construct a **reasoned** argument, make substantiated judgements and reach valid conclusions
	effectively organise and present information **clearly**, supported with **relevant** examples and analysis
	comment **effectively** on strengths and limitations
	link together **appropriate** principles and concepts from the sector
E	The student will be able to:
	demonstrate **acceptable** use of terminology
	demonstrate **basic** understanding of ideas, processes and procedures, applied to **some** familiar and unfamiliar contexts
	use **some** simple mathematical skills relevant to the sector
	limited analysis of information, ideas and research
	construct a **limited** argument, make **appropriate** judgements and reach **some** valid conclusions
	organise and present information supported with **rudimentary** examples and some **acceptable** analysis
	comment on strengths and limitations

Grade	Demonstration of attainment
	put together **some** principles and concepts from the sector

Occupational specialism components

The occupational specialism components are graded distinction, merit, pass and ungraded.

Occupational specialism grade descriptors

Grade	Demonstration of attainment
Distinction	The evidence is logical and provides an **excellent** response to the demands of the **brief.**
	Makes use of relevant knowledge and is **well-informed** by the practices of the sector.
	Demonstrates an understanding of the different perspectives/approaches associated within the sector.
	Makes **excellent** use of facts/theories/approaches/concepts.
	Demonstrates **comprehensive use of** breadth and depth of knowledge and understanding.
	Consistently selects **appropriate** skills/techniques/methods.
	Identifies information from a **range** of suitable sources and makes use of appropriate information/appraises relevancy of information.
	Combines information to make **accurate** and **appropriate** decisions.
	Makes **sound** judgements/takes **appropriate** action/seeks clarification and guidance.
	Successfully tackles both routine **and** non-routine problems that reflect real life situations in the sector.
	Effectively demonstrates skills and knowledge of the relevant concepts and techniques reflected in the sector and is applied across a variety of contexts.
	Tackles unstructured problems that have not been seen before, using their knowledge to analyse and find **suitable** solutions to the problems.
	Analyses data/information in context and applies **appropriate analysis** in confirming or refuting conclusions and carrying out further work to evaluate conclusions.
	Justifies strategies for solving problems, giving clear explanations for their reasoning.

Grade	Demonstration of attainment
Pass	The evidence is logical and a **good** response to the demands of the brief.
	Makes use of relevant knowledge and is **generally** informed by the practices of the sector.
	Demonstrates an understanding of **some** perspectives or approaches associated within the sector.
	Makes **good** use of facts/theories/approaches/concepts.
	Demonstrates breadth and depth of knowledge and understanding.
	Generally selects appropriate skills/techniques/methods.
	Identifies information from appropriate sources.
	Makes use of appropriate information/appraises relevancy of information.
	Combines information to make **accurate** decisions.
	Makes **generally sound** judgements/takes appropriate action/seeks clarification and guidance.
	Able to **successfully tackle routine problems** and make **some progress** on solving non-routine problems in real life situations.
	Demonstrates **most skills and knowledge** of the relevant concepts and techniques reflected in the sector and is applied across different contexts.
	Able to **make some progress** on unstructured problems that have not been seen before, using their knowledge to find solutions to problems.
	Makes **some** justification for strategies for solving problems, giving explanations for their reasoning.

"Threshold competence" refers to a level of competence that:

- signifies that a student is well-placed to develop full occupational competence, with further support and development, once in employment
- is as close to full occupational competence as can be reasonably expected of a student studying the TQ in a classroom-based setting (for example, in the classroom, workshops, simulated working and (where appropriate) supervised working environments)
- signifies that a student has achieved the level for a pass in relation to the relevant occupational specialism component

U grades

If a student is not successful in reaching the minimum threshold for the core and/or occupational specialism component, they will be issued with a U grade.

Awarding the final grade for each component of the TQ

Each core component's marks will be combined to form the overall grade for the core component.

The marks from the occupational specialism assignment will form the occupational specialism grade.

These grades will be submitted to the Institute for Apprenticeships and Technical Education who will issue an overall grade for the T Level study programme.

Calculating the final grade for the T Level programme

To be awarded an overall T Level grade, a student must successfully pass both components of their TQ, complete an industry placement, achieve level 2 English and mathematics if they have not already achieved this prior to starting a T Level, and meet any other requirements set by the Institute's T Level panel. T Levels will vary in size, largely dependent on the size of the TQ, and on whether a student needs to continue to study English and mathematics.

The full list of Functional Skills/GCSE/other alternative qualifications which meet the English and mathematics requirement for T Levels, including details of flexibility for students with SEND, is published in the Specification of apprenticeship standards for England (SASE), which is available via the Department for Education's (DfE) website.

The overall grade for the T Level programme is based on a student's performance in the TQ and would reflect:

- the comparative size of the core component and the occupational specialism
- the grades achieved for the core component (A* to E) and the occupational specialism (P/M/D)

This grading approach also makes it possible to recognise exceptional achievement, through the award of an overall distinction* grade for students that achieve an A* for the core component and a distinction in their occupational specialism.

The following table shows how the core component and occupational specialism grades are aggregated to produce an overall result for this T Level programme:

Core component 50%/occupational specialism 50%:

Core component grade	Occupational specialism grade: Distinction	Merit	Pass
A*	distinction*	distinction	distinction
A	distinction	distinction	merit
B	distinction	merit	merit
C	merit	merit	pass
D	merit	pass	pass
E	pass	pass	pass

Overall T Level grade

This matrix shows the overall TQ grade when both TQ components are combined. For example, if a student achieved a B grade in the core component assessment (indicated by the vertical column on the left) and a merit grade in the occupational specialism assessment (indicated by the horizontal top row), they would achieve a merit grade for the overall T Level programme:

Core component grade	Occupational specialism grade: Distinction	Merit	Pass
A*	distinction*	distinction	distinction
A	distinction	distinction	merit
B	distinction	merit	merit
C	merit	merit	pass
D	merit	pass	pass
E	pass	pass	pass

merit

Section 3: Frameworks

General competency framework

Technical qualifications are required to contain sufficient and appropriate English, mathematical and digital content to help students reach threshold competence in their chosen specialism. As such, a framework of competencies has been developed which awarding organisations are required to use and embed in all technical qualifications (where appropriate).

General English competencies	General mathematical competencies	General digital competencies
GEC1. Convey technical information to different audiences	GMC1. Measuring with precision	GDC1. Use digital technology and media effectively
GEC2. Present information and ideas	GMC2. Estimating, calculating and error spotting	GDC2. Design, create and edit documents and digital media
GEC3. Create texts for different purposes and audiences	GMC3. Working with proportion	GDC3. Communicate and collaborate
GEC4. Summarise information/ideas	GMC4. Using rules and formulae	GDC4. Process and analyse numerical data
GEC5. Synthesise information	GMC5. Processing data	GDC5. Be safe and responsible online
GEC6. Take part in/lead discussions	GMC6. Understanding data and risk	GDC6. Controlling digital functions
	GMC7. Interpreting and representing with mathematical diagrams	
	GMC8. Communicating using mathematics	
	GMC9. Costing a project	
	GMC10. Optimising work processes	

The following table identifies the English, mathematical and digital competencies that we have embedded in skills throughout this technical qualification. The tutor may also teach competencies that are not listed here, where they naturally occur, but these will not be subject to assessment.

English, mathematics and digital competencies relevant to the digital support service technical qualification

General competencies	Core skills	Digital infrastructure	Network cabling	Digital support
English				
GEC1	CS1, CS2, CS3	S2.1, S2.2, S2.6, S3.4, S3.5	S2.1, S2.7, S2.9, S2.10, S3.4, S3.5	S2.2, S2.6, S2.7, S3.4, S3.5
GEC2	CS1, CS2	S2.6	S2.1	
GEC3	CS1, CS2, CS3, CS4	S2.2, S3.4, S3.5, S3.6	S2.1, S2.6, S2.7, S2.9, S2.10, S3.5, S3.6	S2.6, S3.5, S3.6
GEC4	CS1, CS4	S1.4, S1.5, S1.6, S2.1, S2.2, S2.6, S3.1, S.3.2, S3.3	S1.4, S1.5, S2.7, S2.9, S2.10, S3.1, S.3.2, S3.3	S1.4, S1.5, S1.6, S1.7, S2.2, S2.6, S2.7, S3.1, S.3.2, S3.3
GEC5		S1.1, S1.3, S2.2, S3.4, S3.5	S1.1, S1.3, S2.7, S3.4, S3.5	S1.1, S1.3, S3.4, S3.5
GEC6	CS1, CS2			S2.7
Mathematics				
GMC1		S2.5	S2.1, S2.7	
GMC2	CS2	S2.2, S2.5, S2.7	S2.1	S2.2
GMC3		S2.7		S2.2
GMC4			S2.6	
GMC5	CS2, CS3	S1.6, S3.4, S3.6	S1.4, S2.1, S2.6, S3.4, S3.6	S1.6, S2.2, S2.7, S3.4, S3.6
GMC6	CS4	S1.5, S2.2, S3.5, S3.6	S1.5, S3.5, S3.6	S1.5, S2.3, S2.7
GMC7			S2.1, S2.5	
GMC8		S3.6	S2.7, S3.6	S3.6
GMC9				
GMC10	CS1, CS2, CS3, CS4	S2.2	S2.9, S2.10	S1.7, S2.6

General competencies	Core skills	Digital infrastructure	Network cabling	Digital support
Digital				
GDC1	CS1, CS2, CS3, CS4	S1.1, S1.4, S2.3, S2.4, S3.1	S1.1, S3.1	S1.1, S1.4, S1.7, S2.1, S2.2, S3.1
GDC2	CS1	S3.3	S3.3	S3.3
GDC3	CS1	S1.2, S3.4, S3.5, S3.6	S1.2, S2.1, S3.4, S3.5, S3.6	S1.2, S2.2, S2.4, S2.7, S3.4, S3.5, S3.6
GDC4	CS1, CS3, CS4	S1.5, S1.6, S2.6, 3.6	S1.4, S1.5, S2.7, S3.6	S1.5, S1.6, S2.4, S2.6, S2.7, S3.6
GDC5	CS1, CS2, CS4	S1.1, S1.3, S2.2, S3.2	S1.1, S1.3, S3.2	S1.1, S1.3, S1.7, S2.4, S3.2
GDC6	CS2	S1.1, S1.4, S2.3, S2.4	S1.1, S2.2, S2.4	S1.1, S1.4, S1.7, S2.1, S2.2, S2.5

Section 4: TQ content

This section provides details of the structure and content of this qualification.

Qualification structure

The technical qualification (TQ) in digital support services has 2 components:

- core component, comprising route core, pathway core and core skills
- occupational specialism components:
    - Digital infrastructure
    - Network cabling
    - Digital support

The core content is divided into 12 route core elements, 3 pathway core elements and 4 core skills, all of which indicate the relevant knowledge and understanding of concepts, theories and principles relevant to all occupations within digital support services. The knowledge and skills are all externally assessed through written examinations and an ESP.

The occupational specialisms are divided into performance outcomes, each of which indicates the knowledge and skills required to enable students to achieve threshold competence in the chosen occupational specialism. These performance outcomes are all externally assessed through synoptic assignments, in which the student will be expected to demonstrate required knowledge and skills.

Delivery of content

The content does not have to be taught in a linear fashion. However, providers must pay attention to when the assessments are due to take place to ensure that all of the mandatory content (all elements and performance outcomes) has been taught to their students prior to sitting the assessments.

What you need to teach

This section contains all of the mandatory teaching content that underpins the knowledge and skills. The content provided in some cases may not be exhaustive, and providers may wish to teach beyond what is included in the specification to support the student's knowledge and understanding.

English, mathematics and digital competencies have been integrated and contextualised within the skills, throughout the qualification content. These competencies are mandatory and subject to assessment and must be delivered alongside the subject-specific content. The tutor may also teach competencies that are not listed in this specification, but these will not be subject to assessment.

Route core elements

Route core element 1: Business context

What you need to teach

The student must understand:

R1.1 Types of organisations and stakeholders within the business environment.

Organisation types:

- public
- private:
  - small or medium-sized enterprise (SME)
  - large enterprise
  - non-governmental organisation (NGOs)
- voluntary/charity:
  - not for profit

Stakeholder types:

- internal:
  - end users:
    - owners
    - board of directors
    - employees
    - departments
- external:
  - customers/consumers - purchases goods and services
  - clients - engages professional services
  - direct/indirect competitors
  - outsources services and suppliers
  - shareholders
  - investors
  - funders
  - government:
    - local

What you need to teach

- national
- international

Business environments:

- business to consumer (B2C)
- business to business (B2B)
- business to many (B2M)

R1.2 Key factors that can influence the business environment:

- political factors (for example cross party focus and agendas)
- economic factors (for example interest rates, consumer trends, periods of recession)
- social factors (for example social mobility, market trends, cultural expectations, socioeconomic aspects)
- technological factors (for example emerging technologies)
- legal factors (for example legislation changes and updates)
- environmental factors (for example carbon footprints, digital waste)

R1.3 The measurable value of digitalisation to a business:

- sales and marketing:
  - enhanced market research
  - increased opportunities for brand promotion
  - increased communication and coverage via social media
  - online opportunities for selling/e-commerce
  - tracking and management of customer/service-user retention
  - digital analytics (for example customer satisfaction scores)
- operations:
  - enhanced communication channels
  - automation of internal systems
  - remote working functionality
- finance:
  - increased fiscal performance
  - increased reporting options and functionality
  - reduced operating costs

What you need to teach

- key performance indicators (KPIs):
  - easier to monitor

R1.4 The influence and impact of digitalisation within a business context and market environment:

- brand differentiation:
  - brand values
- virtualisation/cloud solutions:
  - enabling scalable, elastic computing solutions to meet business demand
- digital innovations:
  - business intelligence and insight
  - unique selling points (UPS)
- processes and business models:
  - digital manufacturing
  - financial
  - research
- wider access to:
  - customer base
  - range of product and services
- contextualising customer behaviour:
  - digital personalisation
  - platform interoperability
- open standards:
  - using non-platform specific digital identity

R1.5 The role of technical change management in digital operational integrity:

- preparation and planning:
  - innovations within digital technology
  - effectively communicating the rationale for the change
  - communicating the benefits of the change
  - getting ‘buy in’ from all areas of the business who the change effects
- operations:
  - interaction of new or upgraded tools and processes into current digital ecosystem

What you need to teach

- establishing best practice for use of new or upgraded tools and processes
- facilitating processes and business models
- applying fixes

R1.6 The components of technical change management:

- change advisory board (CAB):
  - prioritise change requests
  - review change requests
  - monitor change process
  - provide feedback
- request for change:
  - viability:
    - financial
    - resource
  - analysis of benefits of implementing change request
  - stages of approval
- setting SMARTER objectives:
  - specific
  - measurable
  - achievable
  - realistic
  - time-bound
  - evaluate
  - re-evaluate
- risks:
  - resistance to change from staff/teams
  - misuse of the new tools and processes
  - inadequate support, infrastructure or resource
  - change stalling or impeding workflows
  - knowledge management and single sources of dependencies
- impact:

What you need to teach

- forecasting the impact of change implementation on the operational environment
- measuring positive and negative impact
- analysis of positive and negative impact

- configuration of digital system impacted by the change:
  - current and proposed
- rollback planning - recovering to a previous stable configuration:
  - back-up methodology
  - local
  - cloud
  - disaster recovery planning
- reproducibility:
  - replicating change across other departments or businesses
  - test environment:
    - servers and software
- traceability:
  - responsibility
  - accountability
  - auditing
- document:
  - maintaining up-to-date information
  - recording of all decisions
  - retaining change documentation
  - user training manuals
  - version control

R1.7 Factors that drive change and a range of methods organisations can apply in response to change.

Internal factors:

- restructuring

What you need to teach

- expansion/growth
- downsizing
- new strategic objectives

External factors:

- political:
  - shift in governmental priorities (for example Brexit, international trade deals)
  - change in government
  - war
- economic:
  - meeting new funding/revenue streams
  - recession
  - inflation
  - consumer trends
- social:
  - change in human behaviour (for example birth rates)
  - market/social trends (for example rise in online shopping)
  - socioeconomic aspects
  - remote working
  - cultural expectations
- technological:
  - emerging technologies
  - innovation/efficiency
  - artificial intelligence
  - new payment methods
- legal/regulatory:
  - new legislation
  - changes/updates to legislation (for example national minimum wage, working hours, General Data Protection Regulation (GDPR)/Data Protection Act (DPA) 2018)
  - removal of European Union (EU) legislation
- environmental:

What you need to teach

- sustainability
- reduction in carbon footprint
- green energy
- digital/tech waste
- pandemic

- competitors:
  - new product/service
  - entering new markets

Methods to respond to change:

- new or amended:
  - policies (for example updated health and safety, due to changes in legislation)
  - business processes (for example implementation of new digital technologies)
  - products or services (for example innovation for new markets)
- new or improved digital systems for hardware and/or software (for example DVLA system, NHS referrals, online banking)
- training needs analysis
- restructuring of priorities and resources

R1.8 The steps organisations take to respond to change:

- planning for change:
  - setting budgets and timescales
  - communicating the change activity to all stakeholders
  - clarifying resources required (for example hardware, software, staffing)
- managing change implementation:
  - monitoring progress during implementation of change
  - maintaining quality of service during change
  - business acceptance and compliance with change
  - team upskilling and development to facilitate the change
  - communicating outcomes of change
  - post-project reviews
- reinforcing change:

What you need to teach

- reinforcement planning:
  - checking change is implemented
  - what steps to take if change isn't implemented quickly enough
- collating and analysing outcomes of change data
- monitoring change

R1.9 The measurable value of digital service to customers and end users.

Value to customers:

- efficient digital support for products and services
- timely response to customer queries or needs:
  - communicating expected response time
  - communicating any changes in response and reasons why
- financial savings (for example product/service price comparisons)
- access and engagement:
  - multi-platform multimodal format (for example social media, chat, email, phone)
  - time saving
- social integration for user and support community

Value to end users:

- efficient first line, second line and third line digital support to internal staff
- efficient resolution of end user needs
- effective hardware or software deployment

R1.10 The considerations and value of meeting customer and end user needs within a business context.

Considerations to meet customer and end user needs:

- customer or end user profile:
  - cultural awareness/diversity
  - inclusivity
  - accessibility
  - adhering to guidelines, policies and regulatory requirements
  - level of technical knowledge and skills (for example use of technical terminology)
- customer or end user issues:
  - problem type and pain points:

What you need to teach

- usability
- functionality
- training on new systems

- system or service response time
- system or service availability

Value of meeting customer and end user needs:

- increased financial benefit due to customer retention and satisfaction
- user experience
- reputational:
  - protection of brand reputation
  - brand awareness
  - positive media exposure
- quantitative and qualitative market research
- product development through product use analytics
- more sophisticated marketing allowing personalised and targeted advertisements for consumers
- positive third-party reviews (for example unboxings, meta critic, user reviews)

R1.11 Risks and implications within a business environment.

Risks:

- privacy:
  - potential loss of control over personal and business information
- security:
  - compromises to the confidentiality, integrity and availability of all business data
- non-compliance:
  - non-adherence to policies, procedures and legislation
- audience exclusion:
  - bias towards a particular demographic
- insufficient business resilience:
  - inability to adapt to disruptions
  - inability to adapt to change
- technical:

What you need to teach

- system not fit for business purpose
- doesn't meet user requirements

Potential impact of risks:

- lawsuits
- dismissal
- fines
- reputational/brand damage
- withdrawal of licence/rights to practise
- loss of job
- loss of business:
  - reduction in sales

R1.12 The purpose and applications of codes of conduct within a business.

Purpose and application:

- ensures that individuals and organisations operate within policies, procedures and legislation:
  - professional practice
  - industry standard
- describes accepted practice for individuals and organisations:
  - confidentiality
  - ethical principles
  - use of equipment and facilities
  - standard working practice
  - access permissions to data and systems
  - supports individual company values

Types of codes of conduct within a business:

- organisational codes of conduct (for example Google, Twitter, code of business conduct (COBC)
- professional codes of conduct (for example British computer society (BCS))
- governmental (for example Technology Code of Practice, Data Ethics Framework)

R1.13 Types of hacker and the implications of hacking and non-compliance with a code of conduct.

Types of hacker:

- white hat/ethical hacker:

What you need to teach

- working on behalf of businesses to test the security of systems or networks using ethical tools, techniques and methodologies
- has permission to engage in social engineering within agreed parameters
- feedback given to businesses on system or network vulnerabilities

- grey hat:
  - accesses systems or networks without malicious intent
  - discloses vulnerabilities to businesses or relevant authority
- black hat:
  - unauthorised access to systems or networks for malicious intent
  - compromises or shuts down security systems or networks
  - unauthorised access to passwords, financial information or other personal data
  - threat actors:
    - hacktivist – motivated by specific cause (for example animal rights)
    - organised crime syndicate – motivated by financial gain
    - nation state – motivated by political agenda

Implications of hacking and non-compliance:

- internal implications:
  - disciplinary action
  - loss of employment
  - restriction of potential employability
  - restricted privileges
- external implications:
  - loss of status with professional bodies
  - prosecution:
    - fines
    - imprisonment
  - reputational damage

Route core element 2: Culture

What you need to teach

The student must understand:

R2.1 How the increasing reliance on digital technology can cause ethical and moral impacts on business and society.

Impacts on business:

- impact on company culture:
  - changes in face-to-face communication (for example remote working, video conferencing)
  - increase in expected productivity and outputs
  - increase reach and scale
  - increase of staff monitoring
  - adaptive working practices
- autonomous operation:
  - dehumanisation of service:
    - loss of jobs
    - loss of human empathy in decision making
  - shift in skill requirements and skills redeployment

Impacts on society:

- loss of privacy:
  - digital footprint
  - surveillance
- changing behaviours:
  - social skills
  - scalable remote engagement, wider peer and professional networks
  - creation and curation of a digital identity
- communication access:
  - resistance to technological change
  - potential isolation:
    - transition to remote communication and services
    - due to lack of digital skills or technology
    - locations (for example limited mobile data coverage)

What you need to teach
○ improved access to information (for example educational, online employment searches, access to 24/7 advice - NHS) **R2.2 The impact of unsafe or inappropriate use of digital technology and mitigation techniques to reduce impact.** Impacts: • psychological: ○ cyberbullying ○ mental health ○ addiction (for example gambling, gaming, social media) ○ stress • physical: ○ posture ○ eye strain ○ repetitive strain injury (RSI) ○ reduction of physical activity ○ disturbed sleep patterns Mitigation techniques: • regulate use of digital technology (for example effects on sleep patterns, effects on mental health, screen breaks) • report misuse to relevant authority (for example platform owners, police) • display screen equipment (DSE) and workstation assessment: ○ equipment (for example footrest, back support, screen filters) • self-exclusion (for example gambling website/app)

Route core element 3: Data

What you need to teach
The student must understand: **R3.1 The fundamental characteristics of data.** Data types:

What you need to teach

- numeric
- text
- media
- geospatial
- temporal
- logical

Sources of data for organisations:

- internal:
  - sales data
  - marketing data:
    - engagement data
  - financial data
  - employee data
  - customer data
  - usage data:
    - traffic data
- external:
  - public (for example open data, repositories)
  - government (for example data.gov.uk)
  - suppliers
  - competitors
  - sector/industry
  - market research
  - repositories

Storing data:

- on-premises:
  - internal databases
  - file structures and formats
  - hard drives:
    - solid state drive (SSD)

What you need to teach

        - hard disk drive (HDD)
      - portable storage devices
      - file servers
      - network-attached storage (NAS) devices
      - storage area network (SAN)
  - cloud storage:
      - file storage
      - object storage
      - block storage
      - elastic cloud/scalable storage
      - cloud-based database services

R3.2 The fundamental functions of information systems and the application of data:

- input - data inputted in preparation for processing
- storage - recording and retention of data on an appropriate format:
    - create/store - retain data records for future use or compliance
    - organise - restructure and rank data in a specific order
- processing - transforming data into meaningful output:
    - analyse - business/digital insight through search queries/criteria
    - update - ensuring data records are up to date
    - remove - removal of data entries where appropriate
    - integrate - integrate different sets of information together
- output - data generated by the information system:
    - read/search - identify and find specific information
    - insight - gain from processing to support decisions
- feedback loop - a system structure that allows output to influence future input

R3.3 The concepts and tools of data modelling.

Concepts:

- hierarchical database model - data organised and accessed in hierarchy structure
- network model - data organised and accessed through nodes and links
- entity relationship model - data organised and accessed through use of relationships

What you need to teach

Tools and their application:

- entity relationship diagram (ERD):
  - used to design relational databases
- data flow diagram (DFD):
  - level zero and level one
  - visual representation of information flow within a system

R3.4 The concepts involved in data entry and maintenance.

Data entry:

- assign common data types to screen input boxes:
  - numeric:
    - integer
    - float
    - double
  - text:
    - strings
    - char
  - Boolean
    - true/false
- reducing risk of data entry errors:
  - validation - check that user-entered data is sensible and in correct format
  - verification - check that user-entered data is accurate
- privacy:
  - compliance with standards and legislation for usage and storage

Data maintenance:

- user:
  - editable data screens for permitted data changes
- system administrator:
  - privileges to allow direct changes to data:
    - user level
    - user group level

What you need to teach

- file level

Business resource considerations for data entry and maintenance:

- operational:
  - time
  - staffing
- financial:
  - budget
  - estimating and forecasting
- technological:
  - hardware
  - software
  - storage

R3.5 Characteristics of data formats and importance for analysis.

Data formats:

- file-based structure:
  - data held within one file
  - consistent set of attributes, data types and validation
  - context is held within the file
  - data is referenced within the file
  - data stored in flat file format
- directory-based structure:
  - data held across multiple files
  - contains multiple attributes, data types and validation
  - context held within the file and the structure
  - relational data is referenced across multiple files
  - datasets are extracted from system and filtered
  - data can be structured in a hierarchy system
  - allows multiple data owners and sources
- relational database systems:
  - data organised using normalisation to reduce redundancy

What you need to teach

- data connect by relationships
- structured query language (SQL)/data processing language
- server-client implementation

Importance for analysis:

- easier to query
- easier to keep up to date
- supports with drawing conclusions
- allows sharing of data

R3.6 Methods of presenting and visualising data and their suitability for application.

Presenting data:

- reports
- digital slides
- webinars
- extended reality (XR):
  - virtual reality (VR)
  - augmented reality (AR)
- video
- sound
- animation

Visualising data:

- graphs (for example bar, line)
- charts (for example pie, funnel, area)
- data tables
- dashboards
- infographics
- maps
- heat maps

Suitability for application:

- formal or informal
- meeting requirements:

What you need to teach

- brief
- audience
- level of technical knowledge and skills (for example use of technical terminology)

R3.7 Applications of data within an organisation:

- analysis:
  - identifying trends and patterns
  - monitoring performance:
    - staff
    - product/service usage
  - forecasting (for example predictive analytics)
  - informing decision making
- marketing:
  - customer profiles
  - targeting customers
  - direct promotion
- operational management:
  - monitoring and control of operations
  - setting and monitoring of KPIs
  - service improvement

R3.8 Types of data access management across platforms within in a digital environment.

Types of data access management:

- user access controls:
  - physical access
  - remote access
  - permissions
  - authentication
- application programming interface (API):
  - set of rules or specifications
  - allows interface between software

R3.9 Types and application of access control methods:

What you need to teach
• role-based access control (RBAC) - restricts or allows access to resources based on the role of a user • attribute-based access control (ABAC) - restricts or allows access based on attributes or characteristics • 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

Route core element 4: Digital analysis

What you need to teach
The student must understand: **R4.1 The characteristics and applications of algorithms in digital analysis:** • algorithms - a process or set of clearly defined rules followed to support calculations or problem solving. Characteristics of algorithms: • finiteness - finite number of steps • unambiguous - steps must be clear and lead to one meaning • clearly defined inputs and outputs • logical sequencing of steps • iteration - repetition of steps until results achieved • selection - input leading to choice of step • structured English Applications of algorithms for digital analysis: • automate calculations to improve efficiency of a process • design a step by step solution to solve a problem • supports machine learning for data analysis **R4.2 The process of computational thinking and tools applied in problem solving and algorithm design.** Process of computational thinking: • decomposition - breaking down a complex problem or system into manageable components • pattern recognition - identification of patterns within problems

What you need to teach

• abstraction - analyse information, filter and remove unnecessary detail
• action:
  ○ sequence - order of processes
  ○ selection - execution only when conditions met
  ○ iteration - repetition until conditions met
Tools for problem solving and algorithm design:
• decomposition diagram
• flowchart
• pseudo code

Route core element 5: Digital environments

What you need to teach

The student must understand:
R5.1 Components of physical computing systems and their applications:
• chassis – to house the components of a system
• optical drive – CD/DVD reader and writer
• mainboard/motherboard – allows internal devices to communicate
• central processing unit (CPU) – main computing part of unit
• random access memory (RAM) – volatile temporary storage
• graphics processing unit (GPU) – enables the ability for output to display unit
• storage (for example SSD/HDD) – used to store data
• fans – used to maintain the temperate of computing system
• redundant array of independent disks (RAID) card – controls the level of redundancy used on storage drives
• peripherals:
  ○ screen
  ○ keyboard
  ○ mouse

What you need to teach

R5.2 Types and applications of networks, hardware and software, and the functions of internet of things (IoT).

Networks:

- personal area network (PAN) – single peer-to-peer connectivity (for example wireless headset to a computer)
- local area network (LAN) – interconnected devices belonging to the same organisation within one area (for example within an office building)
- metropolitan area network (MAN) – 2 or more interconnected LANs within a small geographical area (for example buildings at opposite ends of town)
- wide area network (WAN) – many interconnected LANs over a large geographical area (for example the internet)
- virtual private network (VPN) – used to create a secure connection between a device and a network or between different networks (for example working from home device connecting to corporate network using provided VPN)

Hardware:

- switch – provides connectivity to multiple network devices
- router – used to route traffic between networks
- network interface devices:
    - peripheral component interconnect (PCI) network cards
    - universal serial bus (USB) network cards
- cabling:
    - copper
    - fibre optic
- wireless access point – used to deliver wireless networking to capable devices:
    - servers

Software:

- system software:
    - operating systems (OS):
        - proprietary (for example Microsoft Windows, Apple MacOS)
        - open source (for example Linux, Unix)
        - network operating system (NOS)
    - file management utilities

What you need to teach

- application software:
  - productivity suites (for example Video editing)
  - protection software (for example firewall, anti-virus)
  - web browsers (for example Chrome, Firefox, Edge)

Function of IoT:

- devices dedicated to basic services, data collection, manipulation or analysis, requiring servers to process the task and information:
  - data collection, analysis and manipulation:
    - edge computing
    - sensors (for example temperature sensors, vibration sensors)
  - network utilisation
  - use within an industrial context
  - use within a smart city context
  - use within a domestic context (for example, home-based)

R5.3 The types and applications of protocols used to create networks and network referencing models.

Protocols:

- web protocols – applied to web communication (for example retrieving websites):
  - hypertext transfer protocol (HTTP)
  - hypertext transfer protocol secure (HTTPS)
- mail protocols – the ability to send and receive emails:
  - simple mail transfer protocol (SMTP)
  - post office protocol (POP)
  - internet message access protocol (IMAP)
- routing protocols – used to route data between networks:
  - routing information protocol (RIP)
  - open shortest path first (OSPF)

Network referencing models:

- open systems interconnection (OSI):

What you need to teach

- used in troubleshooting - standardised approach to computing system with an underlying structure characterised by 7 layers:
  - physical
  - data
  - network
  - transport
  - session
  - presentation
  - application

- transmission control protocol, internet protocol (TCP/IP):
  - set of communication protocols used by the internet and computer systems characterised by 5 layers:
    - physical
    - data
    - network
    - transport
    - application
      - file transfer protocol (FTP)
      - secure file transfer protocol (SFTP)
      - dynamic host configuration protocol (DHCP)
      - domain name system (DNS)

R5.4 The components and benefits of virtual computing systems.

Components:

- virtual machines (VMs):
  - clients (for example virtual PC, virtual switch, virtual router)
  - servers
- hypervisor:
  - type 1 (for example Microsoft Hyper-V, VMware ESXI)
  - type 2 (for example virtual PC, virtual server, VMware Workstation)

Benefits:

What you need to teach

- more cost effective in larger digital environments
- easier to manage and maintain larger environments
- resilient (for example clustering)
- environmental (for example lower carbon footprint)
- disaster recovery options
- efficient testing environments
- education and training platform

R5.5 The types, services and benefits of cloud computing.

Types of cloud:

- private
- public
- community
- hybrid

Cloud services:

- (infrastructure as a service (IaaS):
  - applications, OS and data are client managed
  - servers, network infrastructure and storage are vendor managed
- platform as a service (PaaS):
  - applications and data are client managed
  - servers, network infrastructure, storage and OS are vendor managed
- function as a service (FaaS):
  - functions are client managed
  - network infrastructure vendor managed
- software as a service (SaaS):
  - access to application software
  - no installation or maintenance
  - client only managed user
  - rest is managed by the vendor
- everything as a service (XaaS):
  - outsourcing all organisational digital requirements

What you need to teach

Benefits of cloud computing:

- cloud portability - ability to quickly and easily move services
- cloud sourcing - purchasing services from a third party using the cloud
- elastic cloud - on-demand services which can be scaled to meet needs
- storage - no physical limitations on storage capacity
- cost effective - efficiencies of scale

R5.6 The methods and benefits of creating a resilient digital environment.

Methods of creating a resilient digital environment:

- installation of software updates/upgrades
- replacement and removal of hardware
- adding redundancy into systems
- decommission and remove legacy hardware and software
- device hardening:
  - removing unneeded applications, ports, permissions and access
  - limiting user account functions
- maintaining effective back-up systems:
  - on-premises
  - off-site/remote
  - cloud
- appropriate and reviewed standard operating procedures (SOPs)
- structured staff training for:
  - new hardware/software
  - staff inductions
  - new and updated policies and procedures

Benefits of a resilient digital environment to the organisation:

- increased security:
  - secure transfer of data
  - secure storage of data
  - reduced system vulnerabilities
  - reduced probability of targeted cyber attacks

What you need to teach

• increased reputation and profile:
  ○ customer confidence
  ○ protects brand image
• lower downtime of services

Route core element 6: Diversity and inclusion

What you need to teach

The student must understand:
R6.1 The principles of digital inclusion, and legislation relating to equality and diversity.
Digital inclusion principles:
• ensuring no one is disadvantaged by a digital system
• checking for bias within datasets before use
• access:
  ○ technology
  ○ connectivity
  ○ conforming to codes of best practice (for example Web Content Accessibility Guidelines (WCAG))
• technical knowledge and skills
Legislation:
• the Equality Act 2010:
  ○ direct discrimination
  ○ indirect discrimination
  ○ 9 protected characteristics:
  ▪ age
  ▪ disability
  ▪ gender reassignment
  ▪ marriage and civil partnership
  ▪ pregnancy and maternity

What you need to teach

- race
- religion or belief
- sex
- sexual orientation

- the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
- the Equality and Human Rights Commission (EHRC) Statutory Code of Practice for 'Services, Public Functions and Associations' under the Equality Act

R6.2 The business benefits of diversity and inclusion:

- more innovative products
- greater appeal to potential employees
- inclusive products
- ability to connect authentically to black, Asian and minority ethnic (BAME) groups
- reduce risk of reputational damage from non-inclusive products

R6.3 Approaches to addressing demographic imbalance in the digital sector:

- increasing cultural awareness of different types of bias
- application of digital inclusion principles
- inclusion by design of digital technologies and systems
- government initiatives
- inclusive recruitment

R6.4 How digital inclusion affects individuals and organisations in the digital sector.

Effects of digital inclusion:

- individuals:
  - inclusive services
  - increased career opportunities
  - enhanced access and connectivity to digital technology
  - greater social mobility
  - greater scope of communication and collaboration
- organisations:
  - greater variation in employment demographics
  - enhanced connectivity in more remote communities

What you need to teach
○ creating and expanding commercial markets ○ greater profitability ○ more innovation ○ more skilled workforce ○ more inclusion resulting in greater employee retention Adverse effects when principles of digital inclusion are not applied: • individuals: ○ reduced quality of life ○ social isolation ○ restriction in services ○ financial loss • organisations: ○ lack of skilled people for required roles ○ lack of innovation ○ breach of legalisation and regulations ○ restriction in services ○ financial loss ○ reputational damage ○ breach of regulations

Route core element 7: Learning

What you need to teach
The student must understand: **R7.1 The advantages of personal and professional development in the digital sector:** • increased industry and sector competence and knowledge • increased employability potential and employment security • achieving accreditation to specific professional disciplines • maintaining currency and relevance to industry

What you need to teach

- achieving access to specific professional bodies
- knowledge of and adherence to industry standards

R7.2 Areas of emerging technology and innovative applications within a commercial and domestic context:

- new mediums for storing information (for example DNA data storage)
- quantum computing/internet and quantum cryptography
- IoT
- artificial intelligence
- XR:
  - AR
  - VR
  - mixed reality (MR)
- blockchain
- application of 3D printing
- 5G
- drones

R7.3 Types of reflection and creativity techniques and how they influence practice within the digital sector.

Reflection techniques:

- Kolb's Experiential Learning Cycle - 4 stages of reflecting on experience:
  - concrete – learning from feelings or experiences
  - reflective – learning from watching
  - abstract – learning from reflections and thinking
  - active – learning from practical application of ideas
- Gibbs' Reflective Cycle - 6 stages of reflecting on experience:
  - description – recording key components of the task or project (for example expected outcome, actions taken, data of occurrence)
  - feelings – recording reactions and feelings
  - evaluation – reviewing positive and negative actions and outcomes
  - analysis – reflecting on process and outcomes of task or project
  - conclusion – summarising actions and outcomes from task or project

What you need to teach

- action plan – recording future plans and areas for improvement

- Boud, Keogh and Walker's model - 3 stages of reflecting on practice:
  - experience – considering behaviour, ideas and feelings
  - reflective – returning to and re-evaluating experiences
  - outcomes – gaining new perspectives or changes in behaviour creativity technique

Creativity technique:

- design thinking:
  - identify users' needs
  - empathise with users' needs
  - define the problem
  - hypothesise
  - map/challenge assumptions
  - ideate - create ideas that might solve the problem
  - prototype feedback loop
  - conduct qualitative research with users
  - validate/disprove assumptions
  - iterate prototype based on research

R7.4 Sources of knowledge within the digital sector and the factors that need to be considered when assessing the reliability and validity of a source.

Sources of knowledge:

- forums
- textbooks
- academic papers
- white papers
- supplier literature
- search engines
- websites
- blogs
- wikis
- social media

What you need to teach
• conferences • developer kits • e-learning • subject matter expert Reliability and validity factors: • author expertise • bias • evidence • subjectivity • context • intended audience • date of publication • corroboration of sources • citations

Route core element 8: Legislation

What you need to teach
The student must understand: **R8.1 Legislation and regulation requirements applied across sectors in a digital context.** UK requirements: • Health and Safety at Work etc Act 1974 (including Work at Height Regulations 2005, Manual Handling Operations Regulations 1992, Management of Health and Safety at Work Regulations 1999, Health and Safety (Display Screen Equipment) Regulations 1992): o key features: ▪ adequate training of staff ▪ adequate welfare provision for staff at work ▪ a safe working environment that is properly maintained ▪ suitable provision of relevant information, instruction and supervision • Investigatory Powers Act 2016:

What you need to teach

- key features:
  - enhances powers for law enforcement and security agencies to obtain and intercept communications and data
  - highlights the way in which new powers are authorised and overseen
  - ensures powers are fit for the digital age
- Freedom of Information Act 2000:
  - key features:
    - public sector are required to publish information
    - members of the public are entitled to request information from public authorities
- Computer Misuse Act 1990
  - key features:
    - governs unauthorised access to computer programmes or data
    - governs unauthorised access with further criminal intent
    - governs unauthorised modification of computer material
- Digital Economy Act 2017:
  - key features:
    - regulation of communication infrastructure and services
- Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations 2018:
  - key features:
    - to make clear the level of accessibility required across websites or applications
- Copyright, Designs and Patents Act 1988:
  - key features:
    - protects intellectual property rights
    - enables control over the ways in which material can be used
- Waste Electrical and Electronic Equipment (WEEE) Directive 2012:
  - key features:
    - governs the safe and environmentally responsible disposal of electrical equipment
- Human Rights Act 1998:
  - key features:
    - governs an individual's right to privacy

What you need to teach

- governs surveillance

- Data Protection Act 2018:
  - key features:
    - UKs interpretation of GDPR

International requirements:

- European Convention on Human Rights (ECHR) - Article 8:
  - key features:
    - the right to respect for family and private life
- General Data Protection Regulation (GDPR):
  - key features:
    - lawfulness, fairness and transparency
    - purpose limitation
    - data minimisation
    - accuracy
    - storage limitation
    - integrity and confidentiality (security)
    - accountability
    - data security
- Electronic Communications Privacy Act (ECPA) 1986 - USA:
  - key features:
    - protect wire, oral and electronic communications while in transit
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act 2003 - USA:
  - key features:
    - sets rules for commercial emails and gives rights to recipients (for example to unsubscribe)

R8.2 The role of criminal law, industry standards and professional codes of conduct in a digital context.

Criminal law:

- national:
  - maintains order
  - resolves disputes

What you need to teach

- protects individuals and property
- safeguards civil liberty

- international:
  - governs offences committed outside of the UK

Industry standards and professional codes of conduct:

- compliance
- facilitating competition within industry
- promoting innovation
- providing interoperability between new and existing systems
- ensuring security
- ensuring transparency of sectors

R8.3 Where to access industry standards and professional codes of conduct in a digital context.

Industry standards:

- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF):
  - Request for Comments (RFC)
- Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA)
- British Standard (BS)
- Institute of Electrical and Electronics Engineers (IEEE)
- Payment Card Industry Security Standards Council (PCISSC)

Professional codes of conduct:

- British Computer Society (BCS)
- Institution of Analysts and Programmers (IAP)
- Chartered Institute of Information Security (CIISec)

R8.4 The importance of keeping up to date with UK and international legislation and regulations and potential consequences to businesses across sectors of being non-compliant.

Importance:

- protection for business
- protection for customer
- avoiding consequences of non-compliance

What you need to teach

Potential consequences of non-compliance:
• financial:
  ○ fines
  ○ loss of business/income
• legal:
  ○ prosecution
• professional:
  ○ termination of employment
  ○ revoked responsibilities
• reputational:
  ○ brand damage
  ○ customer perception
• sector specific consequences (for example health, education, retail, hospitality)

Route core element 9: Planning

What you need to teach

The student must understand:
R9.1 The principles of project planning.
Identification of project aims and objectives:
• project scope:
  ○ user/client requirements
  ○ business case
• expected outcomes
• stakeholder map
• timeline and deadlines
• linked to organisational strategic objectives
Resource requirements:
• people and skills

What you need to teach

- estimates and costings
- venues/premises
- facilities
- equipment
- hardware and software
- stakeholder engagement

Budgeting:

- accurate estimating and forecasting
- financial contingency planning
- reasonable and documented assumptions

Cost-benefit analysis:

- viability of project
- quantifying the intended deliverables

Project lifecycle:

- timing and scheduling (for example communication plan, reporting schedules)
- work packages to break down deliverables
- milestones
- prioritisation identification
- dependencies identification

Risk and issues management:

- identification
- probability
- impact
- prioritisation
- analysis
- mitigation controls
- contingency planning

Quality management:

- monitoring of project deliverables
- quality assurance

What you need to teach
• quality control • review and audit **R9.2 The consequences of ineffective project planning:** • under-resourced • escalating costs • exceeding timeframes • unable to deliver outcomes • negative environmental impact • health and safety risks • scope creep **R9.3 The application of project planning techniques in a business context.** Techniques: • programme evaluation review technique (PERT) – used to identify and estimate timescales of project activities • critical path analysis (CPA) – used to identify key tasks within a project • work breakdown structure (WBS) – used to break down the scope of a project into manageable work packages • responsible, accountable, consulted or informed (RACI) matrix - used to manage and categorise stakeholders • must have, should have, could have, won't have (MoSCoW) – used to prioritise the requirements of a project

Route core element 10: Security

What you need to teach
The student must understand: **R10.1 Types of confidential company, customer and colleague information:** • human resources: o salaries o benefits/perks

What you need to teach

- employment data:
  - recruitment
  - termination
  - appraisals/disciplinary
- medical information

- commercially sensitive information:
  - sales revenue
  - trade secrets
  - profit margins
  - client/customer details
  - stakeholder details
  - contracts
  - intellectual property (IP)
- access information:
  - passwords
  - multi-factor authentication
  - email accounts
  - phone numbers
  - access codes

R10.2 The importance of maintaining and the consequences of not maintaining confidentiality, integrity and availability (CIA).

The importance of maintaining CIA:

- maintains compliance
- maintains trust with internal and external stakeholders
- promotes positive brand image
- avoids security risks and unauthorised access

The consequences of not maintaining CIA:

- financial:
  - regulatory fines
  - refunds/compensation to customers

What you need to teach

- loss of earnings
- legal:
  - lawsuits
  - termination of contract
- reputational:
  - loss of clients
  - damage to brand

R10.3 The technical and non-technical threats that may cause damage to an organisation:

- technical:
  - botnets
  - denial-of-service (DoS)
  - distributed denial-of-service (DDoS)
  - hacking:
    - cross-site scripting (XSS)
    - password-cracking software
    - SQL injection
  - malware:
    - viruses
    - trojans
    - worms
    - remote access Trojans (RATs)
    - key loggers
    - ransomware
    - spyware
    - adware
  - malicious spam:
    - phishing
    - spear phishing
    - smishing
    - vishing

What you need to teach

- pharming
- buffer overflow

- non-technical:
  - human error
  - malicious employees
  - disguised criminals
  - natural disaster (for example flooding)

R10.4 The technical and non-technical vulnerabilities that exist within an organisation:

- technical:
  - inadequate encryption (for example weak or outdated)
  - out of date:
    - software
    - hardware
    - firmware
- software no longer supported by supplier:
  - compatibility of legacy systems
  - fail-open electronic locks
  - weak passwords (for example default passwords)
  - missing authentication and authorisation
  - exploitable bugs/zero-day bugs
- non-technical:
  - employees:
    - not following policies and procedures
    - competency levels of staff
    - lack of recruitment screening
    - poor data/cyber hygiene (for example not archiving dormant staff accounts and access)
  - physical access controls:
    - inadequate security procedures:
      - door access codes not changed regularly
      - using simple access codes and reusing access codes (for example 1234)

What you need to teach

- no monitoring of access to secure areas
- unnecessary staff access to secure areas

R10.5 The potential impacts of threats and vulnerabilities on an organisation:

- loss of sensitive information
- unauthorised access to the system or service
- overload of the system to affect a service
- corruption of a system or data
- damage to system operations
- disclosure of private information and credentials
- unauthorised access to restricted physical environment
- essential security updates not installed

R10.6 Risk mitigation controls to prevent threats to digital systems:

- National Cyber Security Centre (NCSC) Cyber Essentials:
  - firewall to secure internet connections
  - choose most secure settings for devices and software
  - control access to data and services
  - protection from viruses and malware
  - up-to-date software and devices
- anti-virus and anti-malware software
- firewalls:
  - software
  - hardware
- intrusion detection and prevention systems
- encryption:
  - purpose
  - process
  - protocols
- user access, policies and procedures:
  - permissions
  - IT user policies

What you need to teach

- staff training and CPD (continuous professional development):
  - human firewall
- back-ups:
  - full
  - incremental
  - differential
- software and system maintenance:
  - importance of latest software updates
  - scheduled maintenance
  - interruption to service
- air gaps
- honeypot
- virtual private networks (VPNs)

R10.7 The process and protocols of internet security assurance.

Processes:

- installation and configuration of firewalls:
  - inbound and outbound rules:
    - traffic type rules
    - application rules
    - destination and source rules
- network segregation:
  - VLANs
  - physical network separation
  - offline networks
- network monitoring
- removable media controls
- anti-virus
- managing user privileges
- penetration/vulnerability testing:
  - port scanning

What you need to teach
○ SQL injecting testing ○ Secure Sockets Layer (SSL)/Transport Layer Security (TLS) scanning Protocols: • VPN ○ IPSec VPN ○ SSL VPN • SSL/TLS • SFTP - secure file transfers • secure shell (SSH) - secure connection to devices • HTTPS **R10.8 The interrelationship of components required for an effective computer security system.** Components: • confidentiality, integrity and availability (CIA) • identification, authentication, authorisation and auditing (IAAA) • risk management: ○ threats ○ vulnerabilities ○ impact ○ probability ○ mitigation

Route core element 11: Testing

What you need to teach
The student must understand: **R11.1 The purpose of testing digital components.** Purposes of testing: • functionality • usability

What you need to teach

- compatibility
- accessibility
- customer/client/end user satisfaction
- fault-finding and de-bugging
- impact assessment
- efficiency of individual components
- review accuracy of data
- ensuring desired outcome (for example service or product)
- performance monitoring

Digital components:

- software
- hardware
- data
- interfaces
- test scripts

R11.2 The process of applying root cause analysis to problems.

- define the problem
- collect data relating to the problem
- identify what caused the problem
- prioritise the causes
- identify solutions to the underlying problem
- implement the change
- monitor and sustain

R11.3 Testing methods and their application in the digital sector:

- concept testing:
  - scoping and validating requirements
  - informing decisions before committing time and resources to a project
- usability/audience testing:
  - testing whether the functionality fulfils the desired outcome
  - identifying usability problems

What you need to teach
○ determining user satisfaction with product • stress testing: ○ testing whether a system can function with expected demand by replicating real world load • penetration testing: ○ determining vulnerabilities in a controlled environment ○ authorised attack on systems • black box testing: ○ testing inputs and outputs against expected results ○ measuring the functional requirements of a system • white box testing: ○ testing internal structure of process flows

Route core element 12: Tools

What you need to teach
The student must understand: **R12.1 The application of digital tools and methods in a business context.** Presentation tools: • slide/page presentation software: ○ product demo ○ sales meetings ○ training ○ promotion and marketing (for example expos, speaking at events) • digital infographics: ○ posters ○ leaflets • graphs: ○ sales trends ○ market comparisons

What you need to teach

- dashboards:
  - display/monitor KPIs
  - management information
  - business intelligence

Project management methodologies:

- agile - promotes adaptability through different iterations:
  - frameworks:
    - Scrum
    - Kanban
    - lean
    - sprints
- waterfall - definitive stages that follow on from each other
- spiral
- rapid application development (RAD)

Project management tools and their application:

- Gantt charts - used to measure time scales and milestones of a project
- flowcharts - outlines the logical process for workflow
- stakeholder power interest matrix - visual representation to assess stakeholder priority
- budget sheets - organise and document finances over project lifespan (for example forecasting, expense tracking)

Evaluation tools:

- marketing analytics tools:
  - search analytics
  - social media analytics
- financial analytics tools
- reporting tools
- data mining

R12.2 The application of collaborative communication tools and technologies in business.

Communication tools and technologies:

- intranet

What you need to teach

• shared workspaces:
  ○ online
  ○ on-premises
• shared documents
• discussion threads
• online shared storage
• mark-up:
  ○ track changes
  ○ comments
• video conferencing

The pathway core: Core knowledge and understanding across digital support services

Pathway core element 1: Careers within the digital support services sector

What you need to teach

The student must understand:

P1.1 The range of responsibilities, job roles and skills required of professionals in digital infrastructure:

- responsibilities:
  - installing, testing and maintaining infrastructure components and systems
  - maintaining the efficiency and effectiveness of an organisation's infrastructure
  - communicating digital infrastructure updates and scheduled system changes to end users
  - proactive management of digital services using structured techniques and digital tools to ensure optimum availability
  - recovery and restoration of digital services
  - performance optimisation of hardware, software and network system
  - applying security measures to digital devices and networks
  - incident/problem detection, support and escalation (for example escalation to 3rd line technical support)
  - working to relevant legislation, standards and industry best practice
  - system design and documentation to organisational standards
- job roles:
  - service desk roles (for example technician/operative)
  - 1st line to 4th line (for example analyst/engineer)
  - network engineer
  - server engineer
  - infrastructure technician
- skills:
  - analytical thinking and problem solving
  - using digital monitoring and diagnostic tools:
    - logging and service management systems
    - manage social media (for example wikis, messages)

What you need to teach

- communicating effectively with technical and non-technical staff
- project management and planning:
  - prioritisation of tasks and workload
- collaboration and working as part of a team
- continuous learning, improving and upskilling

P1.2 The range of responsibilities, job roles and skills required of professionals in network cabling:

- responsibilities:
  - installing, termination, testing and certification of copper and fibre network cable infrastructure
  - maintenance of copper and fibre optic cabling
  - identify, locate and repair faults in copper and fibre optic network cabling
  - installation of equipment cabinets, fixtures/fittings and rack-mounting equipment
  - applying physical security measures to network cabling and infrastructure
  - carry out a risk assessment (for example health and safety risk assessment)
  - working to relevant legislation, standards and industry best practice
  - production of clear documentation showing cable route maps, testing and acceptance
  - updating asset registers when physical equipment is deployed
  - updating maintenance logs when equipment is repaired or updated
  - use of service management tools and systems to maintain efficiency and effectiveness through good practice, processes and procedures
- job roles:
  - structured cabling installer/engineer (for example telephony, fibre, data)
  - network surveyor
  - network analyst
  - network installation engineer
- skills:
  - manual handling
  - working at height
  - ability to interpret and follow instructions and plans
  - adaptable approach to work
  - project management and planning

What you need to teach

- prioritisation of tasks and workload
- ability to work alone or as part of a team
- customer service skills
- continuous learning, improving and upskilling

P1.3 The range of responsibilities, job roles and skills required of professionals in digital support:

- responsibilities:
  - providing digital support required by businesses of all sizes and in all sectors
  - identifying the difference between digital application requirements and digital service requirements of users:
    - digital application requirements:
      - supply of software
      - troubleshooting application issues
      - storage quota
    - digital service requirements:
      - information and data access
      - loaning of equipment
      - helpdesk support
      - multi-platform support
  - supporting business needs with appropriate digital services (for example hardware and software)
  - providing digital service by supporting end users to access and operate systems
  - providing 1st line desk side and remote technical support for computer hardware or software for internal and external customers
  - communicating digital support updates and scheduled system changes to end users
  - training end users on new digital applications and systems
  - maintaining an up-to-date asset register and configuration management database
  - incident response, resolution and problem management
  - escalation of issues to technical and external support
  - working to relevant legislation, standards and industry best practice
  - updating and maintaining a knowledge base with known fixes and procedure documentation
  - use of service management tools and systems to maintain efficiency and effectiveness through good practice processes and procedures

What you need to teach

- job roles:
  - 1st line support analyst
  - helpdesk analyst
  - service desk analyst
  - support desk analyst
  - IT support technician
  - desktop support technician
  - digital applications support specialist
- skills:
  - analytical thinking and problem solving
  - using logging systems, digital monitoring and diagnostic tools
  - prioritisation of tasks and workload
  - communicating effectively with technical and non-technical users
  - active listening
  - collaboration and working as part of a team
  - customer service skills
  - continuous learning, improving and upskilling

P1.4 Integrated digital communications responsibilities required in digital support services:

- installing, testing and maintaining integrated digital communications systems and networks (for example telephony, video, instant messaging, email)
- managing availability of integrated digital communications systems
- network configuration, monitoring and optimisation of network performance for communications systems
- applying security measures to integrated digital communications systems and networks
- system design and documentation of organisational standards

P1.5 The types of organisations where digital support services roles exist:

- public:
  - education (for example schools, colleges)
  - government (for example local authority, embassies)
  - healthcare (for example NHS hospitals, surgeries)

What you need to teach
○ emergency services • private: ○ telecommunications (for example BT Openreach, Sky, Virgin Media) ○ IT network installers (for example BT Openreach) ○ IT technical specific (for example Microsoft, IBM) • voluntary: ○ charities (for example British Heart Foundation, Cancer Research, RSPCA) ○ trusts (for example National Trust, Woodland Trust) ○ foundations (for example BBC, Children in Need) **P1.6 The routes into digital support services:** • further education (for example vocational specific) • apprenticeships/work-based learning • higher education (for example degree) • professional/vendor qualifications and employer/industry recognised courses (for example CompTIA, Cisco, BCS) • professional recognition (for example progressing within an organisation)

Pathway core element 2: Communication in digital support services

What you need to teach

The student must understand:

P2.1 Types of communication methods applied to digital support services:

- written – formal and informal
- verbal – formal and informal
- non-verbal (for example body language)

P2.2 Types of communication formats and techniques applied to digital support services:

- formats:
  - telecommunication
  - email
  - incident tickets
  - notifications (for example system updates)
  - instant messenger
  - forum
  - face-to-face conversation
  - digital conferencing
  - presentation
- techniques:
  - troubleshooting
  - active listening
  - reading of body language and facial expressions
  - use of open questioning
  - negotiation
  - conflict handling/de-escalation
  - use of clear and concise language (for example terminology based on audience)

P2.3 Factors to consider when communicating to an audience in a digital support services context:

- target audience
- size of audience
- level of digital knowledge, literacy and experience of the audience

What you need to teach

- requirements of audience:
  - communication format
  - level of detail

P2.4 The relation and interaction between digital support services and technical and non-technical customers/clients/end users:

- verbal support in person or over the phone
- written updates by email or added to a support ticket or system which the user can view
- classroom or individual training and support
- remote support
- screen sharing
- messaging technology
- pre-recorded topic-based e-learning

P2.5 The relation and interaction between digital support services and technical and non-technical managers:

- providing direction, support and route for escalation
- written progress reports
- escalation of issues through a support ticketing system or via email
- verbal updates on progress
- presentation given for a project proposal

P2.6 The relation and interaction between digital support services and technical and non-technical peers/colleagues:

- support and knowledge sharing (for example best practice)
- information, advice and guidance:
  - technical training and resources (for example user guides)
- digital conferencing for collaborative working

Pathway core element 3: Fault analysis and problem resolution

What you need to teach

The student must understand:

P3.1 Fault analysis tools and their applications to identify problems:

- system alerts – to flag when a system condition is outside predetermined parameters
- activity/error logs – record of all interactions and events within network systems
- live traces – to identify any network traffic or activity in real-time
- dashboards – a consolidated visual representation of system condition and performance

P3.2 The purpose and application of organisational frameworks for troubleshooting and problem management:

- problem identification – identify and isolate faults using diagnostic and analytical tools to establish the probable cause
- logging – review fault history, identifying potential trends and issues
- action plan – plan or strategy for repair, restoration and prevention of further issues
- escalation – to an appropriate manager, specialist or external third party
- solution implementation – implement required changes to fix and restore services
- problem closure and review – notify user and document any configuration changes

P3.3 Root cause analysis approaches and their applications within problem management:

- the 5 ‘whys’ – an iterative questioning technique to identify underlying issues and causes
- fishbone diagram – to establish cause and effect by grouping possible causes into various categories
- failure mode and effects analysis (FMEA) – identifies which parts of the process or system are faulty
- event tree analysis (ETA) – to identify consequences of a single failure for the overall system reliability
- Pareto chart – to identify the significance of a number of factors on a particular fault or problem
- scatter diagram – to identify a relationship between 2 factors or variables

P3.4 The principles of incident management (for example Information Technology Infrastructure Library (ITIL®)) models in the context of digital support services:

- detection:
  - report and record the incident
  - investigate and perform analysis to determine the extent and cause of the incident
  - prioritise and categorise the incident
- response:

What you need to teach
○ identify an owner who will have responsibility for the incident ○ resolve the issue and restore service ○ record incident resolution and applied changes • intelligence: ○ record lessons learned, fixes and procedure updates ○ perform in-depth investigation and analysis to identify the root cause of the incident (for example forensic analysis) ○ share lessons learned as input to continual improvement and to reduce risk of incident repetition **P3.5 The requirements for external reporting of faults and problem resolution:** • to comply with relevant legislation, regulations and external standards (for example report to the Information Commissioner's Office (ICO)) • to notify customers and end users of: ○ failures of components/systems ○ data breaches ○ data loss

Route core skills

The employer-set project (ESP) requires that students apply and contextualise core knowledge through the demonstration of the following core skills. Parameters have been provided for each skill in order to define what students must be able to demonstrate to fully satisfy the requirements of the ESP.

Core skill 1: Communicate information clearly to technical and non-technical stakeholders

Route core underpinning knowledge

- Route core element 1: Business context
- Route core element 3: Data
- Route core element 6: Diversity and inclusion
- Route core element 9: Planning
- Route core element 12: Tools
- Pathway core element 1: Careers within the digital support services sector
- Pathway core element 2: Communication in digital support services

The student must be able to:

CS1. Communicate information clearly to a technical and non-technical audience:

- identify stakeholder requirements:
  - technical or non-technical terminology
  - formal or informal
  - digital level of knowledge
- identify key factors to determine scope of communication to meet stakeholder requirements:
  - required format
  - frequency of communications
  - content and context:
    - design and layout
    - level of detail
    - digital inclusion
  - compliance with guidelines
- apply the identified requirements for the communications

The student must be able to:

• select and apply appropriate tools to communicate with stakeholders:
  ○ presentation tools
  ○ project management tools
  ○ collaborative communication tools
• record and document appropriate communications information:
  ○ summarise key points of communication
  ○ process and store data in compliance with relevant legislation and guidelines
(GEC1, GEC2, GEC3, GEC4, GEC6, GMC10, GDC1, GDC2, GDC3, GDC4, GDC5)

Core skill 2: Working with stakeholders to clarify and consider options to meet requirements

Route core underpinning knowledge
• Route core element 1: Business context • Route core element 2: Culture • Route core element 3: Data • Route core element 9: Planning • Route core element 12: Tools • Pathway core element 2: Communication in digital support services

The student must be able to:

CS2. Work with stakeholders to clarify and consider options to meet requirements:
• identify scope of processes and expected outcomes:
  ○ collect data to clarify appropriate details
  ○ estimate budget and timescales
  ○ assess and calculate potential risk to meet requirements
  ○ assess cultural impacts to meet requirements
• analyse options to meet stakeholder requirements

The student must be able to:

• discuss with stakeholders to agree parameters based on analysis of options:
  ○ ask and respond to questions to clarify understanding
  ○ explain and present information using technical language correctly and coherently
  ○ encourage contributions from all stakeholders
  ○ summarise key points of discussion
• identify roles of stakeholders:
  ○ responsibilities
  ○ accountabilities
  ○ consulted
  ○ informed
• systematically organise and accurately record decisions and changes
• gather, process and store all information and data responsibly, in compliance with appropriate regulations and standards
(GEC1, GEC2, GEC3, GEC6, GMC2, GMC5, GMC10, GDC1, GDC5, GDC6)

Core skill 3: Apply a logical approach to solving problems, identifying and resolving faults, whilst recording progress and solutions to meet requirements

Route core underpinning knowledge
• Route core element 1: Business context • Route core element 3: Data • Route core element 4: Data analysis • Route core element 5: Digital environments • Route core element 7: Learning • Route core element 9: Planning • Route core element 11: Testing • Pathway core element 3: Fault analysis and problem resolution

The student must be able to:

CS3. Apply a logical approach to solving problems, identifying and resolving faults whilst recording progress and solutions:
• identify and investigate the scope of the problem
• decomposition of problem into component parts:
  o identify and analyse individual issues
• prioritisation of identified issues
• identify possible solutions
• plan, implement and test possible solutions
• apply appropriate solutions based on tested outcomes
• accurately record progress and outcomes:
  o use technical language correctly to aid understanding of outcomes
  o organise outcomes logically and coherently
• record and store data in compliance with relevant legislations and guidelines:
  o include the appropriate level of detail to meet requirements
(GEC1, GEC3, GMC5, GMC10, GDC1, GDC4)

Core skill 4: Ensure activity avoids risks to security

Route core underpinning knowledge
• Route core element 1: Business context • Route core element 8: Legislation • Route core element 9: Planning • Route core element 10: Security • Pathway core element 3: Fault analysis and problem resolution

The student must be able to:
CS4. Ensure activity avoids risks to security:

The student must be able to:

• identify and record potential risks:
  ○ threats
  ○ vulnerabilities
• assess probability and impact of risk
• calculate the severity and interpret the priority of risk, based on the probability and impact
• identify and apply appropriate risk mitigation controls and components
• record outcomes:
  ○ include the appropriate level of detail to meet requirements
• comply with relevant legislations and guidelines
(GEC3, GEC4, GMC6, GMC4, GDC1, GDC4, GDC5)

Occupational specialism: Digital infrastructure

The numbering is sequential throughout the performance outcome, from the first knowledge statement, following on through the skills statements. The 'K' and 'S' indicate whether the statement belongs to knowledge or skills.

Mandatory content

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

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

Knowledge – What you need to teach

The student must understand:

K1.1 The role and types of preventative business control techniques 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:

Knowledge – What you need to teach

- whitelisting
- blacklisting
- access control lists
- sandboxing
- device hardening
- certificate authority

K1.2 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)

K1.3 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)

K1.4 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

Knowledge – What you need to teach

- 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

K1.5 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)

K1.6 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)

K1.7 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:

Knowledge – What you need to teach

- 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

K1.8 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

Knowledge – What you need to teach

        - 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

K1.9 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

K1.10 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)
    - optical media:
        - compact disc (CD)
        - digital versatile disc (DVD)

Knowledge – What you need to teach

- wireless networks

K1.11 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

K1.12 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

K1.13 Approaches and tools for the analysis of threats and vulnerabilities:

- approaches:
  - qualitative – non-numeric:
    - determine severity using 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

Knowledge – What you need to teach

- 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

K1.14 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

Knowledge – What you need to teach

- 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

K1.15 The purpose of 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)

Knowledge – What you need to teach

- 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)

K1.16 Types of risk response within a digital infrastructure 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

K1.17 The process of penetration testing within digital infrastructure:

- 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

K1.18 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

K1.19 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

Knowledge – What you need to teach

- 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)

K1.20 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:

Knowledge – What you need to teach

- 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)

K1.21 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

K1.22 The relationship between organisational policies and procedures and risk mitigation:

- 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)

Knowledge – What you need to teach

        - 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)

K1.23 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
- 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
- Computer Misuse Act 1990:

Knowledge – What you need to teach

- 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:

- 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
- 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

Knowledge – What you need to teach

- 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 into 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

K1.24 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

K1.25 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

Knowledge – What you need to teach

- 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

K1.26 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

K1.27 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

Knowledge – What you need to teach

- appropriate segregation of devices, networks and resources to reduce the impact of a cyberattack

K1.28 Techniques applied to ensure cyber security for internet connected devices, systems and networks:

- wireless security – WPA2 and use of end-to-end security implemented to monitor access to WiFi 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)

K1.29 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

Knowledge – What you need to teach

- 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

K1.30 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

Knowledge – What you need to teach

- 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

Knowledge – What you need to teach

K1.31 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

Knowledge – What you need to teach

        - 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 – allows 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:

Knowledge – What you need to teach
▪ install correct software

Skills – What you need to teach

The student must be able to:

S1.1 Apply and maintain procedures and security controls in the installation, configuration and support of physical and virtual infrastructure to ensure confidentiality, integrity and availability:

- 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

(GEC5, GDC1, GDC5, GDC6)

S1.2 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

(GDC3)

S1.3 Explain the importance of organisational and departmental policies and procedures in respect of adherence to security:

Skills – What you need to teach

- 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)

(GEC5, GDC5)

S1.4 Install and configure software for network and end user devices (for example servers, desktop computers) to identify and mitigate vulnerabilities:

- 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

(GEC4, GDC1, GDC6)

S1.5 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):

- 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

(GEC4, GMC6, GDC4)

S1.6 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)

Skills – What you need to teach

- 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

(GEC4, GMC5, GDC4)

Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure

Knowledge – What you need to teach

The student must understand:

K2.1 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

K2.2 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

Knowledge – What you need to teach

- BS EN 50174

- wireless bands and channels:
  - 2.4GHZ:
    - 802.11b
    - 802.11g
    - 802.11n
  - 5GHZ:
    - 802.11J
- internet protocol version 4 (IPv4) network and subnets:
  - addressing schemes
  - subnetting
- subnet masks
- internet protocol version 6 (IPv6)):
  - IPv6 address types

K2.3 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/WiFi 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)

Knowledge – What you need to teach

- 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
  - WiFi protected access (WPA) 1, 2, and 3
- antennas:
  - omni-directional
  - directional

Knowledge – What you need to teach
○ 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) **K2.4 The requirements of static prevention 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) **K2.5 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)

Knowledge – What you need to teach

- Waste Electrical and Electronic Equipment (WEEE) Directive 2013 (for example removal or disposal of hardware or network components)

K2.6 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

K2.7 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

K2.8 The advantages and limitation of containers:

Knowledge – What you need to teach

- advantages:
  - require fewer system resources
  - easily deployable due 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

K2.9 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)

K2.10 Service functions and their application within a client-server network environment:

- active directory domain services (AD DS):

Knowledge – What you need to teach

- 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

K2.11 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

K2.12 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

Knowledge – What you need to teach

K2.13 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

K2.14 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

K2.15 The principles of disaster recovery plans (DRPs) and business continuity plans (BCPs):

- key principles:
  - identify:
    - risk
    - operational critical systems
    - requirements (for example resources)
  - analyse:
    - business impact (for example impact on departments, customers, suppliers)
    - maximum downtime
  - design:
    - plan components
  - implement:
    - communication plan
  - measure:
    - test

Knowledge – What you need to teach

- compliance (for example with relevant legislation, policies and procedures)
- review and maintain

K2.16 The different purpose of DRPs and BCPs in the context of digital infrastructure:

- BCP – planning and managing business continuity during a disruptive event:
  - alternative business premises
  - adaptive policies and processes
  - application of alternative technologies
- DRP – restoring normal business operations following a disaster (for example flood):
  - restoring functionality or access
  - replacement of infrastructure resources

K2.17 The stages within a solution lifecycle (SLC):

- 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

Knowledge – What you need to teach

- 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

K2.18 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

K2.19 The principles of solution architecture:

- the importance of reuse
- the importance of documentation

Knowledge – What you need to teach

- 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

K2.20 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

Skills – What you need to teach

The student must be able to:

S2.1 Explain the fundamentals of network infrastructure:

- identify and explain the purpose and application of network infrastructure

Skills – What you need to teach

- summarise and explain, using correct technical language, the benefits of network infrastructure within an organisation
- identify and explain the application of protocols and ports

(GEC1, GEC4)

S2.2 Assess workplace risk in regards to electrostatic discharge (ESD):

- 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

(GEC1, GEC3, GMC2, GMC6, GMC10, GDC5)

S2.3 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

Skills – What you need to teach

- apply appropriate back-up policies and procedures
- implement testing to monitor quality of network:
  - functionality
  - performance
- record all test results to inform network improvements

(GDC1, GDC6)

S2.4 Maintain the effective functioning of physical or virtual networks:

- maintain component parts of physical and virtual networks:
  - server:
    - types (for examples 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

(GDC1, GDC6)

S2.5 Make and test a unshielded twisted pair (UTP) cable to required national and international standards:

- determine purpose of cable:
  - calculate required length
- make:

Skills – What you need to teach

- 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

(GMC2)

S2.6 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

(GEC1, GEC2, GEC4, GDC4)

S2.7 Demonstrate the ability to apply all stages of a solution lifecycle in a digital infrastructure context:

- 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

(GMC2, GMC3)

Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge – What you need to teach

The student must understand:

K3.1 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, 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)

K3.2 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)

Knowledge – What you need to teach

- date of publication (for example if the content is outdated)

K3.3 The factors of bias:

- 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

K3.4 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)

Knowledge – What you need to teach

- 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

K3.5 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

Knowledge – What you need to teach

- personal
- blogs
- community forums
- project management tools (from example issue logs, Gantt charts, Kanban boards, burndown charts)
- policy, process and procedure documents

Skills – What you need to teach

The student must be able to:

S3.1 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

(GEC4, GDC1)

S3.2 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

(GEC4, GDC5)

S3.3 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

Skills – What you need to teach

- apply the selected techniques and use the appropriate tools to support the evaluation
- record the findings of the evaluation for the requirement

(GEC4, GDC2)

S3.4 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

(GEC1, GEC3, GEC5, GMC5, GDC3)

S3.5 Identify and understand bias when using sources of knowledge in a specific digital infrastructure context:

- 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

(GEC1, GEC3, GEC5, GMC6, GDC3)

S3.6 Demonstrate critical thinking within a digital infrastructure context:

- 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

(GEC1, GEC3, GMC5, GMC6, GMC8, GDC3, GDC4)

Occupational specialism: Network cabling

The numbering is sequential throughout the performance outcome, from the first knowledge statement, following on through the skills statements. The 'K' and 'S' indicate whether the statement belongs to knowledge or skills.

Mandatory content

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install and test cabling in line with technical and security requirements
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

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

Knowledge – What you need to teach

The student must understand:

K1.1 Types of preventative business control techniques used 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:
    - whitelisting
    - blacklisting

Knowledge – What you need to teach

- access control lists
- sandboxing
- device hardening
- certificate authority

K1.2 Types of detective business control techniques in protecting the digital security of an organisation:

- detective control techniques:
  - physical:
    - CCTV
    - motion sensors
  - administrative, policies and procedures:
    - logs (for example error logs)
    - review/audit (for example people entering and leaving the facilities)

K1.3 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)

K1.4 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

Knowledge – What you need to teach

- acceptable usage policies

K1.5 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)

K1.6 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)

K1.7 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

Knowledge – What you need to teach

- managing assets across the network and logging changes (for example tagging and logging laptops)
- reporting infrastructure changes to management

K1.8 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

K1.9 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)
  - optical media:
    - compact disc (CD)
    - digital versatile disc (DVD)
- network ports
- wireless networks

K1.10 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

Knowledge – What you need to teach

- back-up procedure
- set-up procedure

- service level agreement (SLA):
  - system availability and uptime
  - response time and resolution timescales

K1.11 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

K1.12 Approaches and tools for the analysis of threats and vulnerabilities:

- approaches:
  - qualitative – non-numeric:
    - determine severity using 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

Knowledge – What you need to teach

K1.13 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 WiFi 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

K1.14 The purpose of 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)

Knowledge – What you need to teach

- quantification of impact on asset value (for example financial loss as a result of downtime)

K1.15 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

K1.16 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

K1.17 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

K1.18 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:
  - 5 cyber essentials controls:
    - boundary firewalls and internet gateways – restricting the flow of traffic in systems

Knowledge – What you need to teach

- 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
- remote monitoring and management (RMM) (for example end user devices)
- anti-virus software – protecting against attacks from established threats

K1.19 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)

K1.20 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:

Knowledge – What you need to teach

- 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

K1.21 The relationship between organisation policies and procedures and risk mitigation:

- 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)

K1.22 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.

Knowledge – What you need to teach

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
- 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
- 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:

- ISO 27001:2017:

Knowledge – What you need to teach

- purpose – certifiable standard for information security management
- applications within digital infrastructure:
  - GDPR/DPA 2018
  - information security
  - information management
  - penetration testing
  - risk assessments

- 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

Knowledge – What you need to teach

- Open Web Application Security Project (OWASP):
  - purpose:
    - implement and review the usage of cyber security tools and resources
    - implement education and training into 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

K1.23 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

K1.24 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

Knowledge – What you need to teach

K1.25 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

K1.26 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 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

K1.27 Techniques applied to cyber security for internet connected devices, systems and networks:

- wireless security – WPA2 and end-to-end security implemented to monitor access to WiFi systems
- encryption
- virtualisation
- penetration testing
- malware protection
- software updates and patches
- internet gateway security and access control

Knowledge – What you need to teach

- data leakage protection
- multi-factor authentication
- single logout (SLO)

K1.28 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

K1.29 The fundamentals of network topologies and network referencing models and the application of cyber security principles:

- topologies:

Knowledge – What you need to teach

- 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

Knowledge – What you need to teach

- 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

K1.30 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:

Knowledge – What you need to teach

- 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 concepts:
    - install correct software

Skills – What you need to teach

The student must be able to:

S1.1 Apply and maintain procedures and security controls in the installation and maintenance of network cabling to ensure confidentiality, integrity and availability:

Skills – What you need to teach

- implement security controls in a business environment in line with NCSC's 'Cyber Essentials':
  - boundary firewalls
  - secure configuration
  - 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

(GEC5, GDC1, GDC6)

S1.2 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

(GDC3)

S1.3 Explain the importance of organisational and departmental policies and procedures in respect of adherence to security:

- 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)

Skills – What you need to teach

(GEC5, GDC5)

S1.4 Conduct a security risk assessment in line with the risk management process for a system (for example in 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

(GEC4, GMC5, GDC4)

S1.5 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 networked equipment and 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

(GEC4, GMC6, GDC4)

Performance outcome 2: Install and test cabling in line with technical and security requirements

Knowledge – What you need to teach

The student must understand:

K2.1 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):

Knowledge – What you need to teach

- IPv6 address types

K2.2 Tools and equipment used for network cabling:

- 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

Knowledge – What you need to teach

K2.3 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

K2.4 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

K2.5 The purpose and components of a network design specification:

- purpose:
  - to provide the technical overview of the components
- components:

Knowledge – What you need to teach

- 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

K2.6 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

K2.7 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

Knowledge – What you need to teach

- 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

K2.8 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

K2.9 Principles of Ohm's law and its application to copper network cabling:

- Ohm's law:
  - 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
- application of Ohm's law to network cabling:

Knowledge – What you need to teach

- 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
- 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

K2.10 Features of copper and fibre media types and their applications:

- copper cable:
  - features:
    - durable
    - easy to handle
    - cheaper installation
    - high bandwidth
    - can provide power - Power over Ethernet (PoE)
  - applications:
    - telephony distribution
    - maximum limit of 90m (permanent links)
    - short run LAN within 100m total distance (channel links)
  - 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):

Knowledge – What you need to teach

- 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

Knowledge – What you need to teach

- 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

K2.11 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)

K2.12 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)

Knowledge – What you need to teach

        - 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)

K2.13 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

K2.14 Types of termination points and their applications:

- 66 block:
    - punch-down connection terminal for telephone systems
    - terminate 22 to 26 solid copper wire

Knowledge – What you need to teach

- 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

K2.15 Standards for copper and fibre cable, their methods of termination and ethernet deployment 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

Knowledge – What you need to teach

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

Knowledge – What you need to teach

- 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

K2.16 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:

Knowledge – What you need to teach

- 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

o 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:
  - o resolution of identified security vulnerabilities:
    - ▪ apply fixes
    - ▪ maintaining compatibility of systems
  - o log all changes to hardware and software:
    - ▪ hardware updates
    - ▪ software updates
  - o inform all necessary stakeholders/users of changes
- monitoring and improving network performance:
  - o network monitoring procedures:
    - ▪ monitor user activity
    - ▪ traffic and load
    - ▪ install network monitoring system (for example packet analysers, firewalls)
    - ▪ track network performance benchmarks
  - o predictive maintenance:
    - ▪ predicting life expectancy of network components and plan to replace
  - o reactive maintenance:
    - ▪ reacting to component failure in a network
  - o run to failure (RTF):

Knowledge – What you need to teach

        - retaining network components until natural failure or upgrade
    - continual service improvements

K2.17 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

Knowledge – What you need to teach

        - dropped datagrams
        - address conflicts
        - missing sequence numbers
    - analysis of performance benchmark

K2.18 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

K2.19 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

Knowledge – What you need to teach

- 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

K2.20 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)
  - British Standards (BS):
    - BS 6701:
      - specification for installation, operation and maintenance

Knowledge – What you need to teach

        - BS 7671:
            - Institute of Electrical and Electronics Engineers (IEEE) Wiring Regulations
    - IEEE:
        - IEEE 802.16:
            - Worldwide Interoperability for Microwave Access (WiMAX)
        - IEEE 802.3 series:
            - standard specification for ethernet
    - International Electrotechnical Commission (IEC):
        - IEC60364:
            - international standard on electrical installations for buildings
    - Telecommunications Industry Association/Electronic Industries Alliance (TIA.EIA):
        - TIA/EIA-586-B:
            - defines cable categories (Cat3, Cat5, Cat5e, Cat6) and their performance tests and procedures
    - International Organization for Standardization/International Electrotechnical Commission (ISO/IEC):
        - ISO/IEC11801:
            - international standard for 'Generic Cabling for Customer Premises', dictates cable class
    - European Norm (EN):
        - EN50173:
            - European standard for generic cabling, consistent with ISO/IEC11801 but includes additional requirements for network cabling
- 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

Knowledge – What you need to teach

- 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)

K2.21 Process and management of the identification of asbestos-containing materials (ACM) are identified during installation work:

- actions required to reduce risk and impact of ACM:
  - 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

K2.22 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

Knowledge – What you need to teach

- 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 example continuity tester, network cabling 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

Knowledge – What you need to teach
▪ delayed payments ▪ failed external audits **K2.23 Impact of poor quality workmanship and non-compliance with network cabling working practices:** • incorrect labelling of circuits, cables and equipment: o increases the difficulty of: ▪ troubleshooting problems ▪ general maintenance ▪ adapting the network for different uses • failure to test all cabling: o damage equipment o premature breakdown o impede services on the network o non-identification of system errors

Skills – What you need to teach

The student must be able to:

S2.1 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

(GEC1, GEC2, GEC3, GMC1, GMC2, GMC5, GMC7, GDC3)

S2.2 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 a meet 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

(GDC6)

Skills – What you need to teach

S2.3 Apply patching to terminate copper and fibre cables (single and multi-mode) in compliance with industry standards:

- 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

S2.4 Demonstrate effective application of networking tools for a specific purpose in a network cabling context:

- 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

(GDC6)

S2.5 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)

Skills – What you need to teach

- test all fixtures and fittings to ensure compliance with legislation, installation and safety requirements
- arrange the equipment to meet the specification within the racks

(GMC7)

S2.6 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 wiremap, cable length):
    - identify the appropriate testing tools
    - apply copper test 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

(GEC3, GMC4, GMC5)

S2.7 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

(GEC1, GEC3, GEC4, GEC5, GMC1, GMC6, GMC8, GDC4)

Skills – What you need to teach

S2.8 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:
  - identification
  - probability
  - impact
  - prioritisation
  - 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

(GMC6)

S2.9 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:
  - identification
  - probability
  - impact
  - prioritisation
  - mitigation
- identify and apply appropriate PPE in compliance with legislation (for example Health and Safety at Work etc Act 1974):
  - 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
  - summarise key information

(GEC1, GEC3, GEC4, GMC10)

Skills – What you need to teach

S2.10 Explain the risk management process that must be applied if asbestos-containing materials (ACM) are identified whilst installation work is being carried out:
• undertake the risk management process to identify risk and record all outcomes:
  o identification – request access to onsite register
  o analysis of probability and impact
  o 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
  o summarise key information
(GEC1, GEC3, GEC4, GMC10)

Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge – What you need to teach

The student must understand:

K3.1 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, 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)

K3.2 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)

Knowledge – What you need to teach

- date of publication (for example if the content is outdated)

K3.3 The factors of bias:

- 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

K3.4 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)

Knowledge – What you need to teach

- 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

K3.5 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

Knowledge – What you need to teach

- personal
- blogs
- community forums
- project management tools (for example issue logs, Gantt charts, Kanban boards, burndown charts):
  - policy, process and procedure documents

Skills – What you need to teach

The student must be able to:

S3.1 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

(GEC4, GDC1)

S3.2 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

(GEC4, GDC5)

S3.3 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

Skills – What you need to teach

- apply the selected techniques and use the appropriate tools to support the evaluation
- record the findings of the evaluation for the requirement

(GEC4, GDC2)

S3.4 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

(GEC1, GEC3, GEC5, GMC5, GDC3)

S3.5 Identify and understand bias when using sources of knowledge in a specific network cabling context:

- 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

(GEC1, GEC3, GEC5, GMC6, GDC3)

S3.6 Demonstrate critical thinking within a network cabling context:

- 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

(GEC1, GEC3, GMC5, GMC6, GMC8, GDC3, GDC4)

Occupational specialism: Digital support

The numbering is sequential throughout the performance outcome, from the first knowledge statement, following on through the skills statements. The 'K' and 'S' indicate whether the statement belongs to knowledge or skills.

Mandatory content

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install, configure and support software applications and operating systems
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

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

Knowledge – What you need to teach

The student must understand:

K1.1 The types of preventative business control techniques 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:
    - whitelisting

Knowledge – What you need to teach

- blacklisting
- access control lists
- sandboxing
- device hardening
- certificate authority

K1.2 The types of detective business control techniques in protecting the digital security of an organisation:

- 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)

K1.3 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)

K1.4 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:

Knowledge – What you need to teach

- standard operating procedure (for example setting alarm system, fire drill)
- employment contracts stipulating codes of conduct
- acceptable usage policies

K1.5 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)

K1.6 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)

K1.7 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

Knowledge – What you need to teach

- 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

K1.8 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

K1.9 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)
  - optical media:
    - compact disc (CD)
    - digital versatile disc (DVD)
  - network ports
- wireless networks

K1.10 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)

Knowledge – What you need to teach

- 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

K1.11 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

K1.12 Approaches and tools for the analysis of threats and vulnerabilities:

- approaches:
  - qualitative – non-numeric:
    - determine severity using 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)

Knowledge – What you need to teach

- 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

K1.13 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
    - WiFi dropouts
    - inaccessible systems
    - VPN not connecting
    - expired passwords
  - device failure and faults (for example laptops, tablets, telephones):
    - hard disk failure
    - RAM failure

Knowledge – What you need to teach

        - 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

K1.14 The purpose of 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)

K1.15 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

K1.16 The process of penetration testing within digital support:

- penetration testing (for example wireless network tests):
    - customer engagement
    - information gathering

Knowledge – What you need to teach

- discovery and scanning
- vulnerability testing
- exploitation
- final analysis and review
- utilise the test results

K1.17 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

K1.18 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:
  - 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)
  - device hardening – removing unneeded programs, accounts functions, applications, ports, permissions and access
  - remote monitoring and management (RMM) (for example end user devices)
  - vulnerability scanning (for example port scanning, device scanning)

K1.19 The purpose and types of encryption as a risk mitigation technique and their applications:

- purpose – to store and transfer data securely using cryptography

Knowledge – What you need to teach

- 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)

K1.20 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

K1.21 The relationship between organisational policies and procedures and risk mitigation:

- organisational digital use policy:
  - standard operating procedures for:

Knowledge – What you need to teach

- 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)

K1.22 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
- Data Protection Act (DPA) 2018:

Knowledge – What you need to teach

- 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

- 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:

- 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
- 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

Knowledge – What you need to teach

- 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 into 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

K1.23 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:

Knowledge – What you need to teach

- applying directory services
- security authentication process
- using passwords and security implications
- identification and protection of data
- maintaining an up-to-date information asset register

K1.24 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

K1.25 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)

Knowledge – What you need to teach

- air gapping

K1.26 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 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

K1.27 Techniques applied to cyber security for internet connected devices, systems and networks:

- wireless security – WPA2 and use of end-to-end security implemented to monitor access to WiFi 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)

K1.28 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

Knowledge – What you need to teach

- 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

K1.29 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

Knowledge – What you need to teach

        - 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:

Knowledge – What you need to teach

- 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

K1.30 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

Knowledge – What you need to teach

        - 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

Skills – What you need to teach

The student must be able to:

S1.1 Apply and maintain procedures and security controls in the installation, configuration and support of end user services to ensure confidentiality, integrity and availability:

- 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

(GEC5, GDC1, GDC5, GDC6)

Skills – What you need to teach

S1.2 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

(GDC3)

S1.3 Explain the importance of organisational and departmental policies and procedures in respect of adherence to security:

- 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)

(GEC5, GDC5)

S1.4 Install and configure software end user devices (for example servers, desktop computers) to identify and mitigate vulnerabilities:

- 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

(GEC4, GDC1, GDC6)

Skills – What you need to teach

S1.5 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

(GEC4, GMC6, GDC4)

S1.6 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:
  - 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

(GEC4, GMC5, GDC4)

S1.7 Demonstrate operating data systems effectively to meet the requirements of business within a digital support context:

- identify and clarify the parameter of requirements
- identify data systems relevant to requirements
- apply appropriate security controls and procedures when operating data systems
- comply with all organisational policies and procedures when operating data systems

(GEC4, GMC10, GDC1, GDC5, GDC6)

Performance outcome 2: Install, configure and support software applications and operating systems

Knowledge – What you need to teach

The student must understand:

K2.1 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

K2.2 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

Knowledge – What you need to teach

- 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

K2.3 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:

Knowledge – What you need to teach

- 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

K2.4 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

K2.5 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)

Knowledge – What you need to teach

- 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

K2.6 The types of end user devices and systems where content management systems can be applied to identify and resolve user problems:

- desktop:

Knowledge – What you need to teach

- thick clients
- thin clients

- cloud workspaces:
  - free cloud workspaces
  - paid licensed cloud workspaces
- mobile devices:
  - tablets
  - smartphones
  - wearable technology (for example smartwatches)
  - e-reader
- laptops
- peripherals:
  - mouse
  - keyboard
  - monitors
  - printers/scanners
  - speakers
  - projectors
  - storage drives
  - magnetic reader/chip reader
  - smart card reader
- IoT:
  - smart buildings:
    - alarm systems (for example fire, security)
    - metres (for example water, power)
    - lighting
  - smart devices:
    - autonomous vehicles
    - TVs

K2.7 Types of operating systems and how they are used in a digital support environment:

Knowledge – What you need to teach

- 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

K2.8 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)

Knowledge – What you need to teach

K2.9 Application installation and configuration concepts in a digital support context:

- system requirements:
  - storage space
  - RAM
  - compatibility
  - processor
  - OS
- hardware configuration:
  - 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:

Knowledge – What you need to teach

- 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

K2.10 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:
    - optical media
    - USB-based/solid state (for example flash drive, hot-swappable drive)
  - network-based:
    - preboot execution environment (PXE)
    - Netboot

Knowledge – What you need to teach

- 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)
  - compact disc file system (CDFS)
  - 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

K2.11 The types of deployment methods and the advantages and disadvantages of their application:

Knowledge – What you need to teach

- 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

Knowledge – What you need to teach

        - 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

K2.12 The steps in creating and deploying disk images:

- creation of a base image file
- creation of customisation or answer file

Knowledge – What you need to teach

- 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

K2.13 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

K2.14 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

K2.15 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

Knowledge – What you need to teach

- 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

K2.16 The process of the configuration of on-premise 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

K2.17 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

K2.18 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)

Knowledge – What you need to teach

- encryption setting and certificates
- authentication

K2.19 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

K2.20 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 1st to 3rd line support
- knowledge management:
  - documentation

Knowledge – What you need to teach

- known fixes
- SOPs
- asset management
- auditing

K2.21 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
  - roll back procedures:
    - roll back device drivers
  - roll back OS update failures
  - roll back updates
- deployment using network tools (for example group policy):
  - locally installed
  - network deployed
  - testing
  - release control

K2.22 The process of asset management and its application in digital support:

- identification and planning:
  - user needs
  - organisational needs

Knowledge – What you need to teach

- 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

K2.23 The purpose and applications of mobile device management (MDM):

- 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

Knowledge – What you need to teach

- 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))

K2.24 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

Knowledge – What you need to teach

- screencasts
- managed learning environments (MLE)
- virtual learning environments (VLE)
- sandboxed environments
- MOOCs

Skills – What you need to teach

The student must be able to:

S2.1 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

(GDC1, GDC6)

S2.2 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

Skills – What you need to teach

- 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

(GEC1, GEC4, GMC2, GMC3, GMC5, GDC1, GDC3, GDC6)

S2.3 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

Skills – What you need to teach

- 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

S2.4 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

(GDC3, GDC4, GDC5)

S2.5 Configure accessories and ports of mobile devices for network connectivity:

- apply mobile device management (MDM) to configure mobile devices to allow:
  - wireless data networks
  - cellular data networks
  - hotspots
  - tethering
  - airplane mode
  - Bluetooth
  - email accounts

(GDC6)

S2.6 Explain the application and benefits of digital solutions to meet specific requirements:

- analyse requirements:

Skills – What you need to teach

- 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

(GEC1, GEC3, GEC4, GMC10, GDC4)

S2.7 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

(GEC1, GEC4, GEC6, GMC5, GMC6, GDC3, GDC4)

Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge – What you need to teach

The student must understand:

K3.1 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, 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)

K3.2 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)

Knowledge – What you need to teach

K3.3 The factors of bias:

- 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

K3.4 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)

Knowledge – What you need to teach

- benchmarking
- corroboration:
  - cross-referencing
- triangulation

- evaluation tools:
  - gap analysis
  - KPI analysis
  - score cards
  - observation reports
  - user diaries
  - scenario mapping
  - self-assessment frameworks
  - maturity assessments

K3.5 The functions of incident and request management systems in communicating information:

- reporting:
  - 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
  - online chat bots:
    - artificial intelligence (AI) responds to commonly asked questions
    - efficient use of digital support resource
- recording requirements:
  - user/customer details
  - issue details
  - resolution
  - time taken
- tracking and communicating progress:
  - visibility on status and escalation

Knowledge – What you need to teach

K3.6 Methods of communication and sharing knowledge and their application within a digital support 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

Skills – What you need to teach

The student must be able to:

S3.1 Identify sources of knowledge and apply factors that legitimise their use to meet requirements in a digital support context:

- identify and clarify the parameters of the requirements
- identify appropriate sources of knowledge (up to 3) (for example search engines, blogs)

Skills – What you need to teach

- 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

(GEC4, GDC1)

S3.2 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

(GEC4, GDC5)

S3.3 Select and apply techniques and tools to support evaluation in a digital support 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

(GEC4, GDC2)

S3.4 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

(GEC1, GEC3, GEC5, GMC5, GDC3)

S3.5 Identify and understand bias when using sources of knowledge in a specific digital support context:

- identify the types of bias (for example confirmation, unconscious)

Skills – What you need to teach

- 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

(GEC1, GEC3, GEC5, GMC6, GDC3)

S3.6 Demonstrate critical thinking within a digital support context:

- 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

(GEC1, GEC3, GMC5, GMC6, GMC8, GDC3, GDC4)

Section 5: TQ glossary

TQ specification

Route core

The core knowledge and understanding across the technical qualification route.

Pathway core

The core knowledge and understanding across the technical qualification pathway.

Occupational specialism core

The requirements for the technical qualification occupational specialism.

Student

The person studying the technical qualification (‘The student must…’).

Tutor

The individual delivering the technical qualification.

Provider

The centre delivering the technical qualification.

Series

Assessments which must be attempted in the same assessment window, for example paper A and paper B of the core examination.

Assessment mode

The assessment mode is how an assessment is made available and/or administered to students. For example a written examination can be administered to students via an on-screen platform or via a traditional paper-based document.

Section 6: Additional information

Annual monitoring visits

Our quality assurance team will monitor all approved TQ providers on an ongoing basis. All providers delivering the TQ will be quality assured at least once a year to ensure that they are delivering in line with required standards. Annual monitoring reviews will be carried out either face-to-face or remotely by quality assurers appointed, trained and monitored by us. Providers will be allocated a quality assurer upon approval. Our quality assurers will complete a report following each annual review to record and share their findings.

Guided learning hours (GLH)

Guided learning is the activity of a student being taught or instructed by – or otherwise participating in education or training under the immediate guidance or supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training.

For these purposes, the activity of 'participating in education or training' shall be treated as including the activity of being assessed, if the assessment takes place under the immediate guidance or supervision of a lecturer, supervisor, tutor or other appropriate provider of education or training.

Total qualification time (TQT)

Total qualification time is an estimate of the minimum number of hours that an average student would require in order to complete a qualification.

TQT comprises:

- the GLH for the qualification
- an estimate of the number of hours a student will likely spend in preparation, study or any other form of participation in education or training, including assessment, which takes place as directed by – but not under the immediate guidance or supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training

Essential skills

While completing this qualification, students may develop the knowledge, understanding and essential skills employers look for in employees. These range from familiar 'key skills', such as team working, independent learning and problem solving, to more tricky-to-measure skills, such as:

- appropriate workplace behaviour and dress
- appropriate interpersonal skills
- communicating with professional colleagues/peers and/or hierarchical seniors
- supporting other aspiring employees

- personal manners
- understanding work practices and how different roles and departments function within an organisation

Recognition of prior learning (RPL)

Recognition of prior learning (RPL) may be applied to the core content only.

Providers may, at their discretion, recognise prior learning if they are satisfied that the evidence provided meets the qualification's requirements.

For more information, please refer to the recognition of prior learning (RPL) credit accumulation and transfer (CAT) policy on the Policies & Documents page on the NCFE website.

Qualification dates

We review qualifications regularly, working with sector representatives, vocational experts and stakeholders to make any changes necessary to meet sector needs and to reflect recent developments.

If a decision is made to withdraw a qualification, we will set an operational end date and provide reasonable notice to our providers. We will also take all reasonable steps to protect students' interests.

An operational end date will only show on the regulator's qualification database and on our website if a decision has been made to withdraw a qualification. After this date, we can no longer accept student registrations.

This qualification has external assessments, which can only be taken up to the last assessment date set by us. No external assessments must be permitted after this date, so students must be entered in sufficient time. Please visit the NCFE website for more information.

Staffing requirements

Providers delivering any of our qualifications must:

- have a sufficient number of appropriately qualified/experienced tutors to deliver the TQ to the volume of students they intend to register
- have experience of delivering level 3 qualifications and preparing students for written and project-based assessments
- ensure that all staff involved in delivery are provided with appropriate training and undertake meaningful and relevant continuing professional development
- implement effective processes to ensure all delivery is sufficient and current. This should include standardisation to ensure consistency of delivery
- provide all staff involved in the delivery process with sufficient time and resources to carry out their roles effectively
- ensure staff have an industry focus when delivering content

Core staffing requirements

Staff involved in the delivery of the core content must be able to demonstrate that they have (or are working towards) the relevant occupational knowledge and/or occupational competence in digital support services at the same level of higher than the qualification being delivered. This may be gained through experience and/or qualifications. Understanding of the wider digital sector would be beneficial, including:

- relevant legislation
- emerging technologies within the digital sector
- industry standard operating procedures
- cloud technologies
- application of digital approaches and solutions to problem solving
- network principles and architecture
- data analytics and how data driven decisions influence business decision making
- project management (specifically within the digital sector)

Occupational specialism staffing requirements

Staff involved in the delivery of the occupational specialism content must be able to demonstrate that they have (or are working towards) the relevant occupational knowledge and/or occupational competence in the relevant occupational specialism area at the same level or higher than the qualification being delivered. This may be gained through experience and/or qualifications, including:

- copper and fibre optic cabling installation, testing and tools
- EIA/TIA standards
- network principles and architecture
- cyber security principles and standards

Resource requirements

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

Core:

• software:
  ○ word processing (for example MS Word, Google Docs)
  ○ presentation (for example MS PowerPoint, Google Slides)
  ○ spreadsheet (for example MS Excel, Google Sheets)

- 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

- 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)
- access to hardware with appropriate specifications (for example PC, laptops, mobile devices)
- access to a web server

Occupational specialism – Digital infrastructure:

- software:
  - appropriate network management software (for example load balancing software)
  - network diagramming software (for example Visio, Packet Tracer)
  - operating systems
  - vulnerability scanning software
  - anti-malware software
  - firewall software
  - remote access software
  - intrusion detection software
  - desktop virtualisation software
- hardware:
  - access to appropriate network architecture devices (for example server, switch, hub, firewalls, load balancer, WAP)
  - access to a range of copper cables
  - access to a range of connectors
  - access to WiFi connectable devices
  - media to support installation and deployment of operating systems
  - computers capable of running virtual machines via a hypervisor
- tools:
  - cabling terminating tools (for example wire cutters, crimping tools)

- cable testing tools (for example network cable tester, tone generator and probe)

Occupational specialism – Network cabling:

- software:
  - Packet Tracer
  - firewall software
  - testing software
- hardware:
  - access to appropriate network architecture devices (for example server, switch, hub, firewalls, load balancer, WAP)
  - access to copper and fibre-optic cable
  - access to digital cameras
  - access to a range of cable connectors
  - patch panel
- tools:
  - cabling terminating tools (for example wire cutters, crimping tools)
  - cable testing tools (for example network cable tester, tone generator and probe)
  - optical loss test set (tier 1)
  - optical time domain reflectometer (tier 2)
  - fibre inspection tool
  - access to telecommunications fixtures and fittings (for example cabinets, trunking)
  - label making machine for labelling cables
  - access to physical access equipment:
    - low level access towers
    - mobile elevating work platforms (MEWPs)

Occupational specialism – Digital support:

- software:
  - appropriate network management software (for example Packet Tracer, load balancing software)
  - operating systems
  - vulnerability scanning software
  - anti-malware software

    - firewall software
    - remote access software
    - intrusion detection software
    - email software
    - instant messaging software
    - screen capturing recording software/equipment
    - collaboration software
- 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)

Customer support team

Our customer support team will support you with approvals, registrations, moderation, external assessment, results and general queries.

Fees and pricing

Fees will be made available to eligible and approved providers.

Training and support for providers

Our curriculum team's primary purpose is to support providers and teaching teams in the delivery of this qualification. There are a number of ways in which we can do this, which include:

- providing tailored one-to-one support at your centre
- delivering 'Teaching the T' events at numerous locations throughout the country
- facilitating on-boarding and content webinars
- signposting you to teaching and learning resources
- providing you with delivery updates on the TQ

The variety of support available includes:

- content structure
- teaching strategies
- SEN guidance
- quality assurance

- assessment preparation and blended learning

Should you wish to discuss your teaching and delivery requirements, please email: curriculum@ncfe.org.uk.

Qualification act sheet

This document outlines the key information of this qualification for the provider, student and employer.

Learning resources

We offer a wide range of bespoke learning resources and materials to support the delivery of this qualification, which include:

- schemes of work
- tutor delivery guides

For more information on the resources being developed for this qualification, please check the qualifications page on the NCFE website.

Equal opportunities

We fully support the principle of equal opportunities and oppose all unlawful or unfair discrimination on the grounds of ability, age, colour, culture, disability, domestic circumstances, employment status, gender, marital status, nationality, political orientation, racial origin, religious beliefs, sexual orientation and social background. We aim to ensure that equality of opportunity is promoted and that unlawful or unfair discrimination, whether direct or indirect, is eliminated both in our employment practices and in access to qualifications. A copy of our diversity and equality policy is available on request.

Diversity, access and inclusion

Our qualifications and associated assessments are designed to be accessible, inclusive and non-discriminatory. We regularly evaluate and monitor the 6 diversity strands (gender, age, race, disability, religion, sexual orientation) throughout the development process as well as throughout the delivery, external quality assurance and external assessment processes of live qualifications. This ensures that positive attitudes and good relations are promoted, discriminatory language is not used and our assessment procedures are fully inclusive.

Reasonable adjustments and special considerations policy

This policy is aimed at anyone who uses our products and services and who submits requests for reasonable adjustments and special considerations. Students who require reasonable adjustments or special consideration should discuss their requirements with their tutor.

The most up-to-date version of the policy can be found on the NCFE website where providers can find details of how to request a reasonable adjustment or special consideration.

Contact us

NCFE

Q6

Quorum Park

Benton Lane

Newcastle upon Tyne

NE12 8BT

Tel: 0191 239 8000*

Fax: 0191 239 8001

Email: tlevelsupport@ncfe.org.uk

Websites: www.ncfe.org.uk

Version 1.5 March 2022

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

Owner: Qualification Development Manager

Change history record

Version	Description of change	Approval	Date of issue
v1.0	Post approval, updated for publication		December 2020
v1.1	Update of section: About this TQ Specification to remove draft information		January 2021
v1.2	Updates to Sections 1 and 4 (Institute reference: ODSR_DSS_002-ODSR_DSS_005)		March 2021
v1.3	Branding updated Updates to Sections 1, 2, 4, 5 and 6 (Institute reference ODSR_DSS_007-ODSR_DSS_034)		September 2021
v1.4	Updates to language relating to GLH in section 2. Updates to resources list in section 6. (Institute reference ODSR_DSS_036-039, ODSR_DSS_036-042-43)	October 2021	January 2022
v1.5	Assessment requirement clarification (ODSR_DSS_117)	December 2021	March 2022