Training Qualifications UK

Part of the AQA group

Alternative Academic Qualifications

Qualification Specification

TQUK Level 3 Alternative Academic Qualification in IT and Computing (Extended Certificate) (RQF)

Qualification Number: 610/5496/3

Version V1

Contents

Go to contents Page >

Introduction

Welcome to TQUK

Training Qualifications UK (TQUK) is an Awarding Organisation recognised by the Office of Qualifications and Examinations Regulation (Ofqual) in England and CCEA Regulation in Northern Ireland.

TQUK offers qualifications which are regulated by Ofqual and, in some cases, by CCEA Regulation. All regulated TQUK qualifications sit on the Regulated Qualifications Framework (RQF) and are listed on the Register of Regulated Qualifications.

Qualifications offered by TQUK are designed to support and encourage learners in developing their knowledge and skills. These qualifications may lead to further study or support progression into higher education. TQUK qualifications also provide opportunities to progress to further qualifications. The TQUK website provides news and updates on upcoming developments.

Centre Recognition

To offer any TQUK qualification a centre must be recognised by TQUK.

The TQUK centre recognition process requires a centre to have in place a number of policies and procedures to protect learners undertaking a TQUK qualification and the integrity of TQUK's qualifications. These policies and procedures will also support a recognised centre's quality systems and help the centre meet the qualification approval criteria.

Recognised centres must seek approval for each qualification they wish to offer.

The approval process requires centres to demonstrate that they have sufficient resources, including suitably qualified and occupationally competent staff to deliver, assess, and quality assure the qualification. Centres must also have access to appropriate support in the form of specialist resources. Qualification approval must be confirmed prior to any assessment of learners taking place.

Go to contents Page >

Qualification Specifications

Each qualification offered by TQUK is supported by a specification that includes all the information required by a centre to deliver the qualification. The specification provides mandatory teaching content and assessment details.

The aim of the qualification specification is to guide centres through the process of delivering the qualification.

It is recommended centres read the qualification specification alongside the documents listed in the mandatory documents section on page 17. TQUK's procedures and policies can be found on the website.

Qualification specifications are also available on the website. If you have any further questions, please contact TQUK for assistance.

Centres must ensure they are using the most recent version of the qualification specification for planning and delivery purposes.

Reproduction of this document

Centres may reproduce the qualification specification for internal use only but are not permitted to make any changes or manipulate the content in any form.

Centres must ensure they use the most up-to-date PDF version of the specification.

Use of TQUK Logo, Name and Qualifications

TQUK is a professional organisation, and the use of its name and logo is restricted. TQUK's name may only be used by recognised centres to promote TQUK qualifications. Recognised centres may use the logo for promotional materials such as corporate/business letterheads, pages of the centre's website relating to TQUK qualifications, printed brochures, leaflets, or exhibition stands.

When using TQUK's logo, there must be no changes or amendments made to it, in terms of colour, size, border or shading. The logo must only be used in a way that easily identifies it as TQUK's logo. Any representation of TQUK's logo must be a true representation of the logo.

It is the responsibility of the centre to monitor the use and marketing of TQUK's logos and qualifications on their materials, as well as on those of any resellers or third parties they may use. TQUK must be made aware of centre relationships with resellers of TQUK qualifications. TQUK must be made aware of any additional websites where the centre intends to use TQUK's name and/or logo. If this information is changed, TQUK should be notified immediately. TQUK is required to monitor centres' websites and materials to ensure that learners are not being misled.

If a centre ceases to be/surrenders recognition as a TQUK centre, it must immediately discontinue the use of TQUK's logo, name, and qualifications from all websites and documents.

Go to contents Page >

Accessibility

TQUK is committed to ensuring that all qualifications and assessments are accessible, inclusive, and non-discriminatory. We ensure that no aspect of this qualification disadvantages any group of learners who share a protected characteristic or introduces unjustifiable barriers to entry, other than those essential to the qualification's intended purpose. Where such features are necessary, they will be clearly stated and justified.

All assessment design processes actively identify and remove unjustifiable barriers that could prevent learners, including those with physical disabilities, from demonstrating their knowledge, understanding, or skills. TQUK monitors and reviews the nine protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation) throughout qualification development to maintain accessibility and inclusivity. This approach promotes positive attitudes and fosters good relations among all learners.

More information can be found in our Equality and Diversity Policy.

For learners seeking guidance on Reasonable Adjustments, please see our Reasonable Adjustment Policy.

Go to contents Page >

Section 1: Qualification Essentials

The Qualification

Alternative Academic Qualifications (AAQs) are associated with specific subject areas routes and have been designed to meet the requirements set by the Department for Education (DfE) following the level 3 educational reforms.

The primary purpose of this qualification is to support learners to progress into higher education.

The TQUK Level 3 Alternative Academic Qualification in IT and Computing (Extended Certificate) (RQF) is regulated by Ofqual and is equivalent to one A Level.

In a typical study programme where an AAQ is studied alongside two A Levels, this qualification is designed to be delivered over two years.

Qualification Purpose

The purpose of the AAQ in IT and Computing is to provide learners with the knowledge and skills necessary to progress to higher education and ultimately to work within the IT and computing industry.

AAQs have been approved by the DfE and are allocated UCAS tariff points. An AAQ Extended Certificate is 360 guided learning hours, equivalent to one A Level and will complement a traditional A Level route. When combined with A Levels as part of a mixed-study programme, AAQs provide learners with a high-quality entry route into higher education.

It provides learners with a strong foundation of knowledge and skills in IT and computing principles that complement theoretical concepts covered in the A Level curriculum. This integrated approach will enable learners to gain a full understanding of academic principles and their practical application. This will, in turn, showcase their ability to apply concepts and techniques and strengthen their university/college applications, giving them a competitive edge.

The qualification seeks to equip learners with knowledge and understanding of the fundamental principles and practices that underpin IT and computing. Learners will develop knowledge and skills in areas such as computing fundamentals, computer programming, cloud computing and storage, cyber security (network threats and vulnerabilities), network security management and data gathering, and website technology.

By undertaking this extended certificate, learners will acquire a diverse set of skills that can be effectively applied to higher education studies. The qualification's breadth ensures learners develop transferable skills that are relevant for pursuing higher-level studies. These skills encompass a broad range of areas and can be utilised across various disciplines and fields of study.

Go to contents Page >

Entry Requirements

There are no formal entry requirements, however, learners should have a minimum of a level two in literacy and numeracy or equivalent.

Although TQUK does not require learners to have prior subject knowledge before registering on the AAQ, having a foundational understanding would support their progress.

Entry to the qualification is at the centre's discretion.

The recommended minimum age for this qualification is 16 years.

What will the learner study as part of this qualification?

Learners will be introduced to the fundamentals of computing, providing learners with a strong foundation in IT principles and applications. Learners will study the internal and external components of a computer, including central processing units (CPUs), memory types, storage devices, and input/output peripherals. The role of operating systems in managing hardware and software is explored, alongside key software applications, including productivity tools, system utilities, and security programs. The theme also introduces learners to data representation, examining how numbers, characters, images, and sound are stored and processed by digital systems.

A key aspect of the qualification focuses on programming and scripting, equipping learners with essential coding skills that are in high demand across multiple industries. Learners will explore different programming paradigms, including procedural, object-oriented, event-driven, and functional programming. They will work with various high-level programming languages, learning how to write, debug, and optimise code. This theme introduces client-side and server-side scripting, helping learners understand the interactions between websites, databases, and web applications.

With increasing cyber threats, cyber security is a crucial component of this qualification. Learners will examine cyber security technologies, network threats, and vulnerabilities, gaining insight into how organisations protect their data and IT systems. They will explore firewall configuration, intrusion detection systems, and encryption techniques to secure networks and prevent cyber attacks. Key topics include network security policies, ethical hacking, and cyber legislation, ensuring learners understand legal and regulatory frameworks such as the General Data Protection Regulation (GDPR) and the Computer Misuse Act.

The qualification also covers network security management, where learners study network protocols, maintenance strategies, and security best practices. This includes managing Virtual Private Networks (VPNs), configuring firewalls, and implementing security updates to ensure robust system integrity. Learners will also develop data analysis skills, using statistical methods such as probability, sequence calculation, and pattern recognition to evaluate network performance and detect anomalies.

The final theme of the qualification allows learners to explore website technologies, standards, and programming languages. Learners will develop responsive web applications using Hypertext Markup Language (HTML) , Cascading Style Sheets (CSS), and JavaScript, gaining experience in front-end and back-end web development. They will examine the principles of UX/UI design, ensuring that websites are accessible, functional, and engaging. The theme also covers database integration, where learners will explore how SQL and NoSQL databases are used to store and retrieve information dynamically.

Go to contents Page >

What knowledge and skills will the learner develop as part of this qualification?

This qualification is designed to provide learners with a strong skillset to support their progression to higher-level studies. They will build transferable skills in areas including written and verbal communication, academic writing, critical thinking and analysis, time management, research, and collaborative working.

Learners will develop specialist skills in the exploration of computer components, processors, hardware, and software. They will gain skills in the selection and use of the most appropriate technologies and devices for specific tasks and applications.

Which A Level subjects will complement this qualification?

The A Level subject areas that will complement the qualification include:

- Business
- Computer Science
- Economics
- Mathematics
- Further Mathematics
- Media Studies
- Physics.

Which Higher Education Courses can this AAQ lead to?

This qualification has been designed to support progression to higher education. It may support entry to a range of degree programmes including:

- Computer Science
- Computing (Networks, Cyber Security and Finance)
- Computer Networking and Cloud Security
- Cyber Security
- Computer Engineering.

UCAS Tariff Points

The qualification will attract UCAS Tariff Points, helping learners progress to higher education. The number of tariff points awarded will depend on the final grade achieved.

The tariff points assigned to this qualification are outlined in the following table:

Grade	UCAS Tariff Points
D*	56
D	48
M	32
P	16

Further details may be found on the UCAS website, where learners can also use the Tariff Calculator to estimate their overall predicted tariff points for this AAQ and A Levels.

Learners should be encouraged to verify individual university entry requirements by visiting the university's website, referring to their admission policies, or contacting their admissions team directly.

Structure and Assessment Approach

Structure

The TQUK Level 3 Alternative Academic Qualification in IT and Computing (Extended Certificate) (RQF) comprises five mandatory units.

Mandatory units

Year	Unit Number	Unit Title	GLH	Assessment Type
1	K/651/5393	Unit 1: Fundamentals of Computing	90	EA
	L/651/5394	Unit 2: Programming	90	NEA
2	R/651/5396	Unit 3: Cyber Security – Network Threats and Vulnerabilities	60	EA
	T/651/5397	Unit 4: Network Security Management and Data Gathering – Technical Support	60	NEA
	Y/651/5398	Unit 5: Website Technology – Scripting and Programming	60	NEA

Assessment approach

The assessment has been designed to ensure validity and its fitness for purpose, aligning with regulatory requirements for Alternative Academic Qualifications.

It is essential that all learners are assessed in English. This ruling also applies to all learner evidence presented for external quality assurance purposes.

Each unit in the AAQ is assessed separately using one of two different assessment methods:

- Examination Assessment (EA):
  - an externally set and marked examination
  - designed to assess the learner's understanding and application of knowledge under controlled conditions
- Non-examination Assessment (NEA):

- an externally set brief that requires the learner to apply their knowledge and skills in a practical or research-based context
- supports the demonstration of critical thinking and independent research skills through structured tasks
- internally marked by a centre's assessors and externally moderated by TQUK.

For specific unit assessment requirements, centres should refer to the teaching content section in this Qualification Specification, from page 18.

Additionally, centres must refer to the Assessment Guidance for the Delivery of Alternative Academic Qualifications document. This essential document provides full instructions for the conduct of the EAs and NEAs and explains TQUK's approach to:

- the administration of both types of assessment under controlled conditions
- internally assessed marking
- standardisation and training
- external moderation.

Synoptic assessment

Whilst this qualification is unitised, there are opportunities for synoptic assessment through the NEA assessments of Units 4 and 5 in Year 2. Underpinning unit-specific content is the application of knowledge and research, project management, problem-solving, and critical thinking skills.

The approach of full compensatory marking and the use of a Uniform Mark Scale (UMS) will also provide an indication of learners' holistic skills, knowledge, and understanding from across the qualification content.

Assessment Delivery

The following table shows the delivery approach for this qualification.

AAQ Extended Certificate Delivery Model										
Year 1										
Unit	**NEA Release**	**Standardisation activities**	**EA Window 1**	**EA Window 2**	**NEA completion, internal marking, retake opportunity**	**Initial external moderation**	**NEA results and feedback**	**NEA resubmission opportunity**	**Final external moderation**	**Results release**
1			Late January/ early February *	Mid-May						Window 1 April Window 2 July
2	September	Between 1 October and 28 February			Until 30 April	Between 1-14 May	Mid-May	Between 30 May and 14 June	Between 15-30 June	July
Year 2										
3			Late January/ early February *	Mid-May						Window 1 April Window 2 July
4	September	Between 1 October and 28 February			Until 30 April	Between 1-14 May	Mid-May	Between 30 May and 14 June	Between 15-30 June	
5	September	Between 1 October and 28 February			Until 30 April	Between 1-14 May	Mid-May	Between 30 May and 14 June	Between 15-30 June	

**** In the first year of delivery, there will be no January assessment window in 2027. Thereafter, two assessment window opportunities for the EA will be available annually.**

**** The results for the full qualification will be confirmed at the end of Year 2 in August to coincide with the release of A Level results.**

Guided Learning Hours (GLH)

These hours are made up of all contact time, guidance, or supervision of a learner by a lecturer, supervisor, tutor, trainer, or other appropriate provider of education or training.

The GLH for this qualification is 360 hours.

Directed Study Requirements

In addition to the guided learning hours, learners are expected to dedicate a certain amount of time to self-study and the completion of their Non-examination Assessment (NEA). This directed study time allows learners to review and consolidate their learning, engage in independent research, and prepare for the assessments.

This additional time spent on independent study and assessment preparation is an essential component of the learning process and contributes to the overall achievement of the qualification.

The directed study for this qualification is 40 hours.

Total Qualification Time (TQT)

The TQT provides an estimate of the overall time a learner will typically take to achieve and demonstrate the required level of attainment for the award of the qualification. The TQT includes both the guided learning hours and the directed study requirements.

For this qualification, the TQT is calculated by combining the guided learning hours and the estimated directed study hours. The TQT reflects the total commitment required from learners to successfully complete the qualification.

The TQT for this qualification is 400 hours.

Grading Overview

The grading structure for the qualification comprises Pass, Merit and Distinction for the component assessments and Pass, Merit, Distinction, and Distinction* for the overall qualification grade.

Please refer to the Grading and Marking section on page 7072, for full details.

Reasonable Adjustments and Special Considerations Policy

Learners who require reasonable adjustments or special considerations should discuss their requirements with their tutors or teachers. Centres must seek approval from TQUK before any adjustments or considerations can be put in place.

The centre should identify any potential difficulties a learner may face in accessing the Examination Assessment and Non-Examination Assessment as early as possible and select appropriate adjustments to ensure accessibility. The centre staff are responsible for ensuring all reasonable adjustments are made and must follow TQUK's process for requesting and implementing adjustments. The centre must ensure that all approved Reasonable Adjustments are applied during the Examination Assessment and Non-Examination Assessment.

For more information, please refer to TQUK's Reasonable Adjustments and Special Considerations Policy, please visit our website.

Course Delivery

Pre-course information

All learners should be given appropriate pre-course information regarding any TQUK qualifications. The information should explain the qualification, the fee, the form of the assessment, and any entry requirements or resources needed to undertake the qualification.

Initial assessment

Centres should ensure that any learner registered on a TQUK qualification undertakes some form of initial assessment. The initial assessment should be used to inform a tutor or teacher of the level of the learner's current knowledge, skills, and any additional specific support requirements the learner may need.

Initial assessment can be undertaken by a tutor or teacher in any form suitable for the qualification to be undertaken by the learner(s). It is the centre's responsibility to make available forms of initial assessment that are valid, applicable, and relevant to TQUK qualifications.

Resource Requirements

TQUK expects centres to provide access to appropriate resources and equipment to facilitate the successful delivery of this qualification.

Centres must ensure that facilities and equipment support a safe and engaging learning environment and align with the mandatory teaching content and outcomes. This must include access to digital resources and appropriate technical support.

We do not provide centres with a prescriptive list of equipment to have in place, nor do we stipulate the specific IT requirements or software packages centres should provide.

Go to contents Page >

Learner Registration

Once approved to offer a qualification, centres must follow TQUK's procedures for registering learners. Learner registration is at the discretion of the centre and in line with equality legislation and health and safety requirements.

Centres must register learners before any assessment can take place.

Staffing Requirements

Centres delivering this AAQ must ensure they appoint individuals who are suitably qualified and competent to carry out their respective roles. It is the centre's responsibility to verify that all appointed personnel possess the necessary expertise and experience to deliver and assess the qualification.

The designated person

The centre must appoint a designated person in a senior leadership role to be responsible for overseeing the administration, delivery, and integrity of assessments.

The designated person could hold the following position:

- Head of Centre
- Principal
- Assistant Principal
- Vice Principal.

The designated person is responsible for ensuring that all staff involved in the teaching, assessment delivery, including administration, supervision, facilitation, management, and quality assurance of the AAQ, comply with this document to maintain the security and integrity of the NEA and EA.

Any failure to comply may lead to a malpractice or maladministration investigation by TQUK.

The designated person may appoint additional non-teaching member(s) of staff to support the administration, delivery, and integrity of assessments.

The additional member(s) of staff could hold the following positions:

- Examinations Manager
- Examinations Officer
- Administrative Assistant.

Tutor/Teacher, Assessor, and Internal Quality Assurer requirements

All members of staff involved with the qualification (assessing or IQA) will need to be occupationally competent in the subject area being delivered. This could be evidenced by a combination of:

- A higher level qualification in the same subject area as the qualification approval request
- Experience of the delivery/assessment/IQA of the qualification requested
- Work experience in the subject area of the qualification.

Staff members will also be expected to have a working knowledge of the requirements of the qualification and a thorough knowledge and understanding of the role of tutors/assessors and internal quality assurance. They are also expected to undertake continuous professional development (CPD) to ensure they remain up to date with work practices and developments associated with the qualifications they assess, or quality assure.

Tutor or Teacher

Tutors or teachers who deliver a TQUK qualification must possess a teaching qualification appropriate for the level of qualification they deliver. This can include:

- Further and Adult Education Teacher's Certificate
- Cert Ed/PGCE/Bed/MEd
- PTLLS/CTLLS/DTLLS
- Level 3 Award/Level 4 Certificate/Level 5 Diploma in Education and Training.

Assessor

Staff who assess a TQUK qualification must possess an assessing qualification appropriate for the level of qualification they are delivering or be working towards a relevant qualification and have their assessment decisions countersigned by a qualified assessor. This can include:

- Level 3 Award in Assessing Competence in the Work Environment
- Level 3 Award in Assessing Vocationally Related Achievement
- Level 3 Award in Understanding the Principles and Practices of Assessment
- Level 3 Certificate in Assessing Vocational Achievement
- A1 or D32/D33.

Specific requirements for assessors may be indicated in the assessment strategy/principles identified in individual unit specifications.

Internal Quality Assurer

Centre staff who undertake the role of an Internal Quality Assurer (IQA) for TQUK qualifications must possess or be working towards a relevant qualification and have their quality assurance decisions countersigned by a qualified internal quality assurer. This could include:

- Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practice
- Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Processes and Practice
- V1 qualification (internal quality assurance of the assessment process)
- D34 qualification (internally verify NVQ assessments and processes).

It is best practice that those who quality assure qualifications also hold one of the assessing qualifications outlined above. IQAs must follow the principles set out in Learning and Development NOS 11 - Internally monitor and maintain the quality of assessment.

Go to contents Page >

Useful Websites

- Office of Qualifications and Examinations Regulation
- Register of Regulated Qualifications

For further details regarding approval and funding eligibility please refer to the following websites:

- Education & Skills Funding Agency for public funding information for 14+ learners in England
- Learning Aim Reference Service (LARS)

Mandatory Documentation

Centres must ensure they read this Qualification Specification alongside the following TQUK policies and guidance documentation:

- Appeals Policy
- Assessment Guidance for the Delivery of the Alternative Academic Qualifications
- Complaints Policy
- Conflict of Interest Policy
- Equality and Diversity Policy
- GDPR and Privacy Policy
- Reasonable Adjustments and Special Considerations Policy
- Malpractice and Maladministration Policy.

Go to contents Page >

Section 2: Teaching and Learning

Teaching Approach

Each unit includes the following information to support its delivery:

- an overview of the unit structure and its assessment approach
- an introduction to the unit and any key considerations that apply
- the mandatory teaching content.
- assessment requirements.

The mandatory teaching content has been structured to provide a clear distinction between the level of breadth and depth of knowledge that the learner must cover. It is presented in the specification as follows:

- **topic:** each subject area is introduced within a light blue box that provides a clear reference point for the content that will be covered
- **breadth:** the introductory "stem" sentence in each assessment outcome outlines the overarching scope of the topic. It defines the key concepts, principles, approaches, and themes that learners are expected to understand. The use of amplification terminology further supports the exploration of the topic
- **depth:** the bullet points following each stem sentence outline the specific details and expectations for learner knowledge and application. All bullet points must be covered, as they define the required level of detail and establish the scope and focus of mandatory teaching, learning, and assessment.

Each unit includes essential information to support effective planning and delivery. We outline the mode of assessment and any required resources, followed by the mandatory teaching content. Additionally, a dedicated assessment approach section specifies key details, including the Assessment Objectives (AOs) tested, important dates, and any specific requirements relevant to the topic.

Centres should inform learners that some topics within qualification specifications and its associated assessments may cover themes that certain learners may find triggering. Centres must be aware that assessment materials may include vocationally relevant content that could be sensitive.

Unit 1: Fundamentals of Computing

Unit number:	K/651/5393		
Level:	3	**GLH:**	90
Unit Introduction:	Modern computing relies on an understanding of different types of computer systems, their internal components, and the software that enables them to function efficiently. From personal computers to large-scale multi-user systems, the choice of hardware and system architecture influences performance, scalability, and functionality. This unit explores the features of various computing systems, including personal computers, mainframes, and hyper-converged systems, highlighting their advantages, limitations, and real-world applications. Key topics covered in this unit include the function and impact of internal components such as the CPU, RAM, storage devices, and motherboards. It examines how these components interact, affecting processing speed, multitasking capabilities, and overall system performance. The role of operating systems in managing hardware, software, and user interactions is also explored, including their functions, advantages, and different types such as single-user, multi-user, and real-time operating systems. This unit also considers security and system management, including the importance of firmware, drivers, and system utilities in optimising performance and ensuring stability. By understanding how computer systems operate and are maintained, learners will develop a strong foundation for working with IT systems, supporting further study in software development, networking, and digital security.		
Assessment Type:	Examination Assessment (EA)		

Teaching content:	
1.1	**Types of computers**
Learners will be able to examine the key features of single-user and multi-user computer systems, assess their advantages and disadvantages, and apply their understanding to identify where each system type would be most appropriate in a given context	

1.1.1	The features of computers:
	
	• single-user systems
	  ○ definition:
	  ▪ general-purpose computer designed for use by an individual
	  ○ features:
	  ▪ single-user system
	  ▪ applications for personal use, for example, email, spreadsheets, web access
	  ▪ can be laptops, tablets, towers, and more complex machines
	• multi-user systems:
	  ○ definition:
	  ▪ computer system that allows multiple users to access the system and run multiple applications simultaneously
	  ○ features:
	  ▪ multiuser accounts
	  ▪ mainframes

Teaching content:	
	▪ supercomputers ○ hyper-converged systems: ▪ Nutanix and Hyperflex ▪ can manipulate large volumes of data: ▪ online bookings ▪ payroll ▪ weather prediction ▪ simulator ▪ multi-processor ▪ use of time-slicing.
1.1.2	Advantages and disadvantages of single-user systems: • advantages: ○ better/high performance ○ flexibility and customisation ○ privacy and security control measures ○ personalised experience ○ better use of shared resource ○ easier data backup • disadvantages: ○ purchase cost ○ running costs ○ harder to maintain ○ harder to gain access to technical support ○ limited collaboration ○ limited scalability ○ higher impact of downtime (planned and unplanned).
1.1.3	The advantages and disadvantages of multi-user systems: • advantages: ○ cost-efficiency: ▪ centralised management: the ability to control, monitor, and administer system resources, user access, security, and operations from a single, central location ▪ easier to share files and resources ○ resource utilisation: ▪ scalability: can upscale storage, memory, computing power, and network capacity ▪ targeted upgrades for necessary components ▪ reduces costs and downtime compared to upgrading the entire system • disadvantages: ○ performance impact ○ security and privacy concerns ○ downtime impacts multiple users ○ central storage of data gives one target for compromise.
1.2	**Internal components of computers**
Learners will be able to identify and explain the functions of key internal computer components, memory types, and operating systems, and understand how these elements work together to execute instructions and manage computing tasks efficiently	
1.2.1	The function of internal components of a Central Processing Unit (CPU): • Control Unit (CU):

Teaching content:	
	○ fetches instructions from memory ○ decodes instructions into a format the Arithmetic Logic Unit (ALU) can understand ○ controls the flow of data within the CPU ○ directs the operations of the ALU, registers, and other components ○ manages the timing and sequencing of operations • Arithmetic Logic Unit (ALU): ○ performs arithmetic operations (addition, subtraction, multiplication, division) ○ performs logical operations (AND, OR, NOT, comparisons) ○ carries out calculations and data manipulation as directed by the CU • main memory: ○ stores data and instructions that the CPU is actively using ○ provides fast access to information needed for processing ○ is volatile, meaning data is lost when power is turned off (Important to distinguish from secondary storage) • registers: ○ small, high-speed storage locations within the CPU ○ hold data and instructions that are being actively processed ○ essential for fast data access and manipulation • cache: ○ a smaller, faster memory that stores frequently accessed data and instructions ○ acts as a buffer between the CPU and main memory ○ improves performance by reducing the time it takes to access data • internal and external buses: ○ internal buses: ▪ connect the various components within the CPU ▪ carry data, addresses, and control signals ○ external buses: ▪ connect the CPU to other components on the motherboard, such as main memory and peripherals ▪ enable communication between the CPU and the rest of the system.
1.2.2	The function of internal components of a computer: • motherboard • Central Processing Unit (CPU) • Random Access Memory (RAM) • Hard Disk Drive (HDD) or Solid State Drive (SSD) • Power Supply Unit (PSU) • Graphics Processing Unit (GPU) • cooling system • Input/output controllers (IO) • Network Interface Cards (NIC) • sound card • optical drives • expansion cards.
1.2.3	The purpose of a motherboard: • connects and integrates hardware components • regulates cooling by using temperature sensors and fans • slots and connectors for CPU, memory, cards, and storage • data transfer between components • power distribution and voltage regulation

Teaching content:	
	• installs peripherals and devices • supports audio, networking, and expansion • Trusted Platform Module (TPM) to store encryption keys.
1.2.4	The properties of a range of memory chips: • Read-Only Memory (ROM): o relatively fast read speeds o non-volatile (data is retained when power is off) o smaller capacity o stores firmware, Basic Input/Output System (BIOS), and other essential instructions for booting the computer o data usually written only once during manufacturing • flash memory: o fast read and write speeds o non-volatile - Does not lose data when power is off o wide range of capacities o used in Universal Serial Bus (USB) drives, memory cards, SSDs, and other storage devices o can be erased and reprogrammed electronically o limited write cycles before degradation o rewritten electronically • cache memory: o very fast read and write speeds o volatile - can lose data when power is off o small capacity o stores frequently accessed data and instructions for the CPU o can be written to and read from very quickly o used for high speed access to frequently used data o dynamically overwritten by CPU o integrated by CPU for rapid access o no significant wear-out concerns • EEPROM (Electrically Erasable Programmable Read-Only Memory): o moderate read speeds, slower write speeds o non-volatile o typically smaller capacity o used to store small amounts of data that need to be updated occasionally, such as BIOS settings o can be erased and reprogrammed electrically • Hard Disk Drive (HDD): o slower read and write speeds compared to SSDs and RAM o non-volatile o large capacities, typically measured in terabytes o primary storage for operating systems, applications, and files o can be written to and read from repeatedly • Solid State Drive (SSD): o very fast read and write speeds o non-volatile o Wide range of capacities, from gigabytes to terabytes o can be used as primary storage or for high-performance applications o can be written to and read from repeatedly • Random Access Memory (RAM): o very fast read and write speeds o volatile o moderate capacity, typically measured in gigabytes

Teaching content:	
	○ stores data and instructions that the CPU is actively using ○ can be written to and read from very quickly.
1.2.5	The functions of operating systems: • input recognition • output device recognition • tracking files and directories • managing peripheral devices • sharing resources between users • ensuring that users do not interfere with each other • managing security • access to devices, programs, and data.
1.2.6	The purpose of file libraries: • file organisation • easy access • grouping of similar files • integration with applications • backup and sync features to prevent data loss.
1.2.7	The process of a Fetch-Execute Cycle: • fetch: ○ the CPU retrieves an instruction from main memory ○ the Program Counter (PC) holds the memory address of the next instruction ○ the instruction is fetched and loaded into the Instruction Register (IR) • decode: ○ the instruction in the IR is decoded by the Control Unit (CU) ○ the CU determines the type of operation to be performed ○ the CU identifies the operands involved in the operation • execute: ○ the Arithmetic Logic Unit (ALU) performs the operation ○ operands are fetched from registers or memory ○ the ALU performs the calculation or data manipulation • memory access: ○ if the instruction involves memory access, this step is executed ○ the memory address is calculated ○ data is read from or written to memory • write-back: ○ the results are written back to a register or memory location ○ the PC is updated • interrupt: ○ signal from hardware or software indicating an event that requires immediate attention ○ CPU checks for interrupts ○ if interrupt is pending, the CPU saves its state and jumps to an interrupt handler to process the event ○ after handling the interrupt, the CPU resumes the interrupted program.
1.3	**Ports and devices**

Teaching content:	
Learners will be able to identify a range of ports, input devices, and external hardware components, explaining their purposes and how they support communication between users, systems, and peripheral technologies across digital environments	

1.3.1	The range of computer ports and their purpose:
	
	• USB port:
	  ○ connects peripheral devices
	  ○ various connector types (A, B, C, Micro)
	  ○ supports different data transfer speeds
	• Secure Digital (SD)/Micro SD card reader port:
	  ○ reads and writes data
	  ○ supports SD and Micro SD cards
	• HDMI port:
	  ○ connects to displays
	  ○ transmits video and audio
	• Ethernet port:
	  ○ connects to wired network without need of adapter
	  ○ for internet access and network communication
	• Audio jacks:
	  ○ connects audio devices
	  ○ for headphones, speakers, and microphones
	• VGA Port:
	  ○ connects to older displays
	  ○ analog video signal
	• DisplayPort:
	  ○ connects to high-resolution displays
	  ○ digital video and audio
	• Serial port:
	  ○ connects older devices
	  ○ primarily legacy use
	• Thunderbolt port:
	  ○ supports high speed data transfer and video output
	  ○ power delivery through single connection.

1.3.2	Purpose and function of common input devices:
	
	• mouse:
	  ○ controls the cursor on the screen
	  ○ used for selecting objects, navigating menus, and drawing
	• keyboard:
	  ○ inputs text and characters
	  ○ used for commands and shortcuts
	• touch screen:
	  ○ allows direct interaction with the screen
	  ○ used for selecting, navigating, and drawing
	• web cam:
	  ○ captures video and still images
	  ○ used for video conferencing, live streaming, and recording
	• microphone:
	  ○ captures audio
	  ○ used for voice input, recording, and communication
	• barcode readers:
	  ○ scans barcodes to retrieve data
	  ○ used in retail, inventory management, and logistics

Teaching content:	

	• graphic tablet:
	  ○ allows for precise drawing and sketching
	  ○ used by artists, designers, and animators
	• (Musical Instrument Digital Interface (MIDI)):
	  ○ connects electronic musical instruments to computers
	  ○ used for recording, sequencing, and controlling musical instruments.

1.3.3	Range of common external devices and their purpose:
	
	• output devices:
	  ○ printers (2D, 3D):
	  ▪ 2D printers produce text and images on flat surfaces
	  ▪ 3D printers create three-dimensional objects from digital designs
	  ○ screens:
	  ▪ display visual information
	  ▪ monitors, TVs, and touchscreens
	  ○ speakers:
	  ▪ Produce audible sound
	  ▪ Play music, voice, and other audio
	  ○ projectors:
	  ▪ project images onto a large surface
	  ▪ used for presentations and entertainment
	  ○ headphones:
	  ▪ provide private audio output
	  ▪ worn on or in the ears
	• storage devices:
	  ○ USB drives:
	  ▪ portable storage using flash memory
	  ▪ connect via usb port
	  ○ SSD:
	  ▪ high-speed storage using flash memory
	  ▪ can be internal or external.

1.4	**Software**
Learners will be able to identify, compare, and evaluate different types of system and application software, including their purpose, benefits, and limitations. They will also explore how software supports key computing functions such as system management, security, user access, and software compliance, and explain how these tools support system functionality, reliability, and security in modern computing environments	

1.4.1	Types and purpose of different software:
	
	• systems software:
	  ○ operating system
	  ▪ types of operating systems:
	  • general purpose
	  • mobile
	  • single user
	  • multi-user
	  • multiprocessing
	• a range of operating systems:
	  ○ Microsoft Windows
	  ○ Apple Mac OSX
	  ○ Android

Teaching content:	
	○ Linux ○ Unix • multitasking (co-operative and pre-emptive) • multi-threading operating systems ○ device drivers: ○ firmware: ▪ types: • BIOS • bootloader • embedded • controller • Internet of Things (IoT) ○ system utilities: ▪ types: • systems backup • systems optimisers • disk formatters • disk defragging • text editor • graphic editor • applications software: ○ types: ▪ word processors ▪ databases ▪ computer games ▪ spreadsheets ▪ email ▪ internet software ○ Approaches to implementation: ▪ bespoke designed for specific client needs, tailored ▪ off-the-shelf adjusted for specific client needs.
1.4.2	The advantages and limitations of shareware, freeware and open-source software: • shareware: a type of software distribution model where users are allowed to evaluate and use a program before purchasing it: ○ advantages: ▪ trial periods ▪ cost-effective ▪ widely available ○ limitations: ▪ limited functionality using trials ▪ time limitations ▪ lack of support unless subscribed • freeware: software that is available for use at no cost to the user: ○ examples: VisualStudio Code Libre Office AVG Security ○ advantages: ▪ no cost ▪ accessible ▪ community support ○ limitations: ▪ limited features

Teaching content:	
	▪ advertisements ▪ lack of updates • open source: software that is made available with its source code, allowing users to view, modify, and distribute the code: ○ examples: ▪ Mozilla Firefox ▪ WordPress ▪ Linux • advantages: ▪ flexibility ▪ community collaboration ▪ able to inspect code to identify issues/vulnerabilities • limitations: ▪ need technical expertise ▪ fragmentation ▪ varying levels of community support.
1.4.3	The role and impact of Systems Management Software (SMS): • infrastructure management ○ optimises resource allocation and workload balancing ○ reduces downtime and improves system efficiency ○ supports scalability • performance enhancement ○ identifies bottlenecks affecting system speed and responsiveness ○ automates routine tasks to reduce manual intervention ○ allocates system resources effectively to prevent overload • security improvement ○ detects vulnerabilities and enforces compliance policies ○ provides real-time threat monitoring and response ○ manages access control and user authentication • failure detection and prevention ○ predicts hardware and software failures before they occur ○ reduces system downtime through proactive maintenance ○ logs and analyses issues to prevent recurring failures • device, printer, and storage monitoring ○ tracks system health and performance metrics in real time ○ ensures storage efficiency and prevents capacity issues ○ monitors networked devices for usage trends and faults • troubleshooting and issue resolution ○ diagnoses system failures through automated logs and alerts ○ facilitates remote management and quick issue resolution ○ reduces it workload by providing data-driven insights.
1.4.4	The role and impact of security software features on system protection: • firewalls: ○ regulates network traffic to prevent unauthorised access and cyber threats ○ strengthens perimeter security but does not protect against internal breaches or encrypted malware ○ varies in effectiveness based on configuration, rule complexity, and network policies • antivirus software: ○ detects, prevents, and removes malware through multiple scanning techniques ○ uses signature-based detection for known threats but requires frequent updates

Teaching content:	
	○ implements heuristic analysis to identify new and evolving threats ○ employs behavioural analysis to monitor system activity and detect suspicious patterns • anti-spyware: ○ prevents unauthorised data collection by removing spyware and tracking software ○ protects against keyloggers, tracking cookies, and browser hijacking ○ enhances privacy monitoring by blocking malicious websites and tracking attempts • authorisation: ○ controls user access levels after authentication, limiting exposure to sensitive data ○ uses Role-Based Access Control (RBAC) and Access Control Lists (ACLs) to enforce security policies ○ implements Multi-Factor Authorisation (MFA) to strengthen identity verification • authentication: ○ confirms user identity before granting access to systems or networks ○ uses Single-Factor Authentication (SFA) for basic access control ○ employs Multi-Factor Authentication (MFA) for enhanced security by requiring multiple verification methods ○ incorporates passwordless authentication to reduce password vulnerabilities • biometrics: ○ provides physical authentication through fingerprint scanning, facial recognition, and iris scanning ○ uses behavioural biometrics such as voice recognition, keystroke dynamics, and gait analysis for additional security layers ○ enhances authentication security by making credentials unique and difficult to replicate • encryption: ○ protects sensitive data by converting it into a secure format requiring a decryption key ○ uses symmetric encryption for fast, efficient security with shared keys ○ applies asymmetric encryption for secure communication using public and private keys ○ implements End-to-End Encryption (E2EE) to protect data across its entire transmission path.
1.4.5	The features of software inventory: • identification: ○ name ○ license ○ product keys • documentation: ○ name ○ version number ○ installation date ○ restrictions • licence compliance: ○ number purchased compared to installations ○ identification of violations • version control: ○ updates ○ patches ○ upgrades

Teaching content:	
	• reporting: ○ analysis of usage and compliance.
1.5	**Introduction to code**
Learners will be able to apply their knowledge to recognise how code operates at a fundamental level. They will assess the methods used to convert source code into machine-readable formats, understand the characteristics of different programming languages, and explore how logical operations and truth tables are applied in computing processes	

1.5.1	The purpose and types of character encoding:
	
	• purpose: tells computers how to interpret digital data into letters, numbers, and symbols:
	  ○ types:
	  ▪ American Standard Code for Information Interchange (ASCII)
	  ▪ Unicode
	  ▪ Unicode Transformation Format (UTF).

1.5.2	Methods to convert source code to machine code:
	
	• assemblers:
	  ○ reads assembly instructions
	  ○ translates them into machine instructions
	  ○ outputs an executable file
	• cross-assemblers:
	  ○ developing software for embedded systems, microcontrollers, or gaming consoles
	• translators and their differences:
	  ○ interpreters:
	  ▪ reads a line of code
	  ▪ translates it into machine code
	  ▪ executes it immediately
	  ○ compilers:
	  ▪ reads the whole program
	  ▪ converts it into an executable file
	  ▪ runs the compiled binary without additional translation.

1.5.3	The characteristics of different types of programming languages:
	
	• natural languages:
	  ○ resemble human communication but lack precision for computational tasks
	  ○ applied in Artificial Intelligence (AI), voice recognition, and Natural Language Processing (NLP)
	  ○ limited adoption due to ambiguity and inconsistent structure
	• human-readable vs computer-readable languages:
	  ○ human-readable languages use structured syntax, improving code clarity and collaboration
	  ○ computer-readable languages execute instructions directly, offering speed and efficiency
	  ○ trade-offs exist between developer accessibility and system performance
	• low-level languages:
	  ○ machine code consists of binary instructions, enabling direct CPU execution but requiring extensive technical knowledge

Teaching content:	
	○ assembly language bridges human understanding and machine operations, using mnemonic codes ○ common in embedded systems, Operating System (OS) development, and high-performance computing where control is essential • high-level languages: ○ use structured commands and logical expressions to simplify development ○ java ensures cross-platform compatibility via the Java Virtual Machine (JVM), making it popular for enterprise applications ○ C++ balances manual memory control with object-oriented capabilities, offering flexibility ○ Hypertext Preprocessor (PHP) specialises in server-side scripting and web applications ○ Python prioritises readability and versatility, widely used in data science, automation, and AI ▪ Supports rapid development and prototyping ▪ There are several AI libraries available to be used with Python • fourth-generation languages (4GL): ○ emphasise simplified, human-like commands for programming ○ SQL manages and queries databases efficiently with declarative syntax ○ designed for business applications, data manipulation, and rapid software development.
1.5.4	A range of logical operations: • AND: ○ the AND operation returns true only if both inputs are true • OR: ○ the OR operation returns true if at least one input is true • NOT: ○ the NOT operation inverts the input – true becomes false, and false becomes true • NAND: ○ the NAND operation returns false only when both inputs are true; otherwise, it returns true • XOR: ○ the XOR operation returns true only if the inputs are different (one is true, one is false).
1.5.5	The purpose and application of truth tables: • defining logical operations: ○ truth tables represent fundamental logic gates ○ they provide a clear, structured way to understand how a logical operation behaves for different inputs • verifying Boolean expressions: ○ check whether two Boolean expression are equivalent ○ simplifying logical expression using Boolean algebra • designing and testing digital circuits: ○ essential in digital circuit design to predict circuit behaviour ○ engineers verify logic gate combinations in CPUs, ALUs, and microcontrollers • debugging and error checking in programming: ○ help test logic conditions in programming ○ ensure decision making logic is correct before implementation • used in AI and decision-making systems: ○ used in expert systems to determine decision rules ○ used in AI decision trees to map logical outcomes.

Teaching content:	
1.6	**Data in computing and IT**
Learners will be able to distinguish between data and information, explore different data types and structures, and understand how data is collected, processed, stored, and applied to support analysis and informed decision-making in IT contexts	

1.6.1	The definition of 'data' and 'information':
	
	• data:
	  ○ elements which can be processed to produce useful information:
	  ▪ numbers (numeric)
	  ▪ characters (alphanumeric)
	  ▪ images
	  ▪ signals
	• information:
	  ○ organised data which delivers knowledge, clarification or proof:
	  ▪ reports
	  ▪ charts
	  ▪ graphs
	  ▪ telephone directories
	  ▪ textbooks.

1.6.2	The benefits and limitations of data types:
	• qualitative:
	  ○ definition:
	  ▪ non-numerical data that describes characteristics, opinions, or categories
	  ○ benefits:
	  ▪ provides rich, detailed insights
	  ▪ captures subjective experiences and context
	  ○ limitations:
	  ▪ difficult to quantify and analyse statistically
	  ▪ potential for bias in interpretation
	• quantitative:
	  ○ definition:
	  ▪ numerical data that can be measured and analysed statistically
	  ○ benefits:
	  ▪ enables objective comparison and statistical analysis
	  ▪ easily measurable and replicable
	  ○ limitations:
	  ▪ lacks depth and context
	  ▪ may not capture subjective or complex factors
	• descriptive:
	  ○ definition:
	  ▪ data that summarizes past events or trends without explaining causes
	  ○ benefits:
	  ▪ efficiently organizes large datasets
	  ▪ helps identify patterns and trends
	  ○ limitations:
	  ▪ only provides an overview
	  ▪ does not explain why patterns occur or predict future outcomes
	• diagnostic:
	  ○ definition:
	  ▪ data analysis that identifies causes of past events or trends
	  ○ benefits:
	  ▪ helps understand why something happened

Teaching content:	
	▪ useful for troubleshooting and improving processes ○ limitations: ▪ requires high-quality data ▪ correlation does not always imply causation • predictive: ○ definition: ▪ uses historical data to forecast future trends and outcomes ○ benefits: ▪ supports proactive decision-making ▪ helps anticipate future needs and risks ○ limitations: ▪ predictions are probabilistic, not certain ▪ relies on historical data, which may not always reflect future conditions • prescriptive: ○ definition: ▪ uses data analysis to recommend specific actions ○ benefits: ▪ provides actionable recommendations ▪ improves efficiency and decision-making ○ limitations: ▪ requires accurate predictive models ▪ complex to implement and may still require human oversight.
1.6.3	The importance of a range of factors in the data collection process: • accuracy: ○ data is correct • reliability: ○ data is consistent • objectivity: ○ free from bias and subjectivity • currency: ○ up-to-date data • context: ○ gives meaning to the data collected • collection technique: ○ methods used to gather data will impact: ▪ quality ▪ relevance ▪ usability • GDPR obligations with personal information handling: ○ compliance with GDPR.
1.6.4	The structure and use of data storage units: • bits and nibbles: ○ bits (binary digits) form the fundamental unit of data, representing values as 0 or 1 ○ nibbles consist of four bits, often used in hexadecimal representation and low-level computing tasks • bytes and their multiples: ○ bytes consist of eight bits, forming the standard unit of data storage ○ kilobytes (KB) store small amounts of data, such as text files and simple program instructions ○ megabytes (MB) handle larger files, including images, documents, and small applications

Teaching content:	
	○ gigabytes (GB) support videos, software installations, and operating systems ○ terabytes (TB) accommodate mass data storage, including server backups and high-resolution media ○ petabytes (PB) are used in data centres, cloud computing, and large-scale analytics • words and common multiples: ○ words represent fixed-size data units processed by a CPU, with size depending on architecture ○ common multiples scale data storage capacity in binary (base-2) or decimal (base-10) formats.
1.6.5	The processes of a range of arithmetic operations: • addition (+): the process of combining two or more numbers to find their total or sum where the plus symbol (+) is used to denote addition • subtraction (-): the process of finding the difference between two numbers, where the minus symbol (-) is used to denote subtraction • multiplication (*): the process of repeated addition or combining equal groups, where the asterisk symbol (*) is used to denote multiplication • division (/): the process of distributing or splitting a quantity into equal parts, where the forward slash symbol (/) is used to denote division.
1.7	**Cloud computing and cloud storage**
Learners will be able to explain the key characteristics, service models, and capabilities of cloud computing, and evaluate the advantages and disadvantages of using cloud-based solutions for data storage, system access, scalability, and operational efficiency	
1.7.1	The characteristics and capabilities of cloud computing: • on-demand self-service: ○ provides instant resource provisioning without manual intervention ○ reduces dependency on its teams for infrastructure management • broad network access: ○ enables access to cloud services via multiple devices and platforms ○ supports remote working, mobile computing, and global connectivity • resource pooling: ○ allocates computing resources dynamically across multiple users and workloads ○ enhances cost efficiency by sharing infrastructure across organisations • rapid elasticity: ○ adjusts resource allocation automatically or manually based on demand ○ prevents performance bottlenecks by scaling computing power as needed • measured service: ○ tracks and optimises resource usage through monitoring and metering ○ supports pay-as-you-go pricing models, reducing operational costs • multi-tenancy: ○ allows multiple customers to share cloud infrastructure securely ○ provides isolation between tenants while maintaining resource efficiency • high availability and reliability: ○ ensures minimal downtime through redundant systems and data replication ○ improves disaster recovery and business continuity strategies • scalability: ○ expands storage, processing, and networking resources based on workload changes ○ supports growth for businesses without requiring hardware investment

Teaching content:	

	• security:
	  ○ implements encryption, authentication, and access controls for data protection
	  ○ provides continuous monitoring and compliance with security standards
	• service models:
	  ○ includes infrastructure as a service (iaaS), platform as a service (paaS), and software as a service (SaaS)
	  ▪ Specific providers include AWS, Azure, Google Cloud
	  ○ offers flexibility in deployment and management of computing resources.

1.7.2	Advantages and disadvantages of cloud computing and cloud storage:
	
	• advantages:
	  ○ cost efficiency
	  ○ scalability and flexibility
	  ○ accessibility
	  ○ high reliability
	  ○ automatic software updates
	  ○ data backup and recovery
	  ○ improved collaboration
	• disadvantages:
	  ○ dependency on internet
	  ○ data security concerns
	  ○ limited control
	  ○ potential downtime
	  ○ bandwidth limitations
	  ○ vendor lock-in
	  ▪ customer becomes highly dependent on one provider's technologies, services, or APIs, making it difficult, costly, and time-consuming to switch to another vendor.

Unit 1: Assessment Approach

The mode of assessment used for this unit is an Examination Assessment (EA). This assessment method is externally set and marked by TQUK, ensuring consistency and reliability in the evaluation of learner's knowledge and understanding.

An overview of the assessment approach is outlined in the table below:

Assessment description	The EA comprises a balance of multiple-choice questions (MCQ), extended-response questions (ERQ) and short-answer questions (SAQ).
Assessment windows	Late January/early February** and early May Centres have the flexibility to timetable the EA within the specified assessment window.
Duration of EA	2 hours

** **Important**: in the first year of delivery, there is no assessment window opportunity in January 2027. Thereafter, EAs will be available annually in late January/early February and mid-May.

The Examination Assessment will be conducted under exam conditions in a controlled environment. Centres must refer to the Assessment Guidance for the Delivery of Alternative Academic Qualifications document available on our website for further information to support the administration of the EA.

The assessment has been carefully aligned with the unit's assessment objectives (AOs) to create a consistent framework for learners. The table below confirms the assessment objectives that will be covered in the Examination Assessment.

Assessment objective	Description
AO1 – Recall knowledge and information	Learners are to **recall** knowledge and information
AO2 – Apply knowledge and information	Learners are to **apply** knowledge and information to questions, problems and scenarios
AO3 – Interpret, analyse or evaluate information, ideas or different viewpoints	Learners are able to **interpret**, **analyse** or **evaluate** information, ideas or different viewpoints to make **judgements** that are reasoned or draw conclusions.

Unit 2: Programming

Unit Number:	L/651/5394		
Level:	3	**GLH:**	90
Unit Introduction:	Programming underpins modern IT and computing, enabling the development of software applications, systems, and digital solutions that support businesses, industries, and individuals. This unit introduces core programming concepts and techniques, covering procedural, object-oriented, and event-driven programming paradigms. Learners will explore programming constructs such as variables, data types, loops, conditionals, and functions, developing a structured approach to problem-solving and software development. A key focus of this unit is understanding the principles of efficient and maintainable code. Topics include code modularity, error handling, debugging, and the use of algorithms and data structures to improve performance. Learners will also examine different programming languages and their applications, including Python, JavaScript, and other high-level languages commonly used in software and web development. This unit provides a foundation in programming logic, syntax, and structure, supporting progression to more advanced topics such as software engineering, web development, and database management. By developing problem-solving and analytical thinking skills, learners will be better prepared to design and implement effective software solutions in a range of IT environments.		
Assessment Type:	Non-examination Assessment (NEA)		

Teaching content:	
2.1	**Computing languages**
Learners will be able to explore the features and use of high-level programming paradigms, particularly in Python, and understand how key programming concepts such as variables, control structures, modularity, and file handling are applied across different language types	
2.1.1	The application of different high-level paradigms with Python: • procedural paradigm • functional paradigm • object-oriented paradigm • event driven paradigm.

2.1.2	The features and applications of computer programming languages:
	• concurrency and multithreading:
	  ○ variable or object types:
	  ▪ Boolean variables
	  ▪ single character
	  ▪ integer
	  ▪ real
	  ▪ strings
	  ▪ arrays
	  ▪ pointers

Teaching content:	
	▪ structures or records ○ variables or objects scope: ▪ global ▪ local ○ declarations ○ statements ○ expressions ○ assignments ○ constructs: ▪ sequence ○ selection: ▪ simple if ▪ nested if ▪ case type statement ○ iteration: ▪ pre-condition loops ▪ post-condition loops ○ modularity and functions: ▪ arguments and parameters ▪ functions with no arguments and no return value ▪ functions with no arguments but do have a return value ▪ functions with arguments but no return value • functions with arguments and a return value ○ data files: ▪ text files ▪ binary files (record) ▪ SV files ▪ JSON files ▪ XML files ▪ database files ○ source files: • valid program statements as defined by the language.
2.2	**Client and server-side language**
Learners will be able to compare the properties and applications of client-side and server-side scripting languages, understanding how each is used to build dynamic, interactive, and data-driven web applications	
2.2.1	Properties of and applications of server-side scripting language: • scripting frameworks and languages: • PHP • Python • Considerations when choosing a framework: • operating system support • commercial reputation • market share and penetration • server-side script elements and syntax: ○ purpose ○ case sensitivity ○ identifiers ○ variables and constants:

Teaching content:	
	▪ (programming and system defined) ○ data types: ▪ integer ▪ decimal ▪ Boolean ▪ string ▪ character ▪ date/time ▪ currency ○ value range ○ declaration and initialisation ○ scope and visibility: ▪ public ▪ private ▪ local (module-level) ▪ global ▪ namespaces ○ data structures ○ array: one-dimensional and multi-dimensional ○ lists, stacks, queues ○ text files, XML files ○ Relational databases: ▪ MySQL ▪ MSSQL ▪ tables, records and fields ○ operators ○ arithmetic ○ relational ○ logical ○ concatenation ○ common language constructs ○ types of access: ▪ command line ○ web-based interface: ▪ phpMyAdmin ○ database client: ▪ Oracle ▪ MySQL ▪ Workbench.
2.2.2	Properties of and applications of client-side scripting language: • types: ○ scripting languages: ▪ JavaScript ▪ VB Script ▪ Adobe ActionScript ○ programming languages: ▪ Java ○ execution environments: ▪ web browser • Java virtual machine (JVM) • limits to client PC access • JavaScript elements and syntax • purposes (adding web page behaviour): ○ change HTML element content via Document Object Model (DOM) ○ change HTML element attributes via DOM

Teaching content:

- change HTML CSS styles via DOM
- validate HTML form input
- add interactive elements, event handling

- declaration section <script></script>
- comments
- case sensitivity
- JavaScript syntax
- external Java script files
- identifiers, variables (local, global) and data types
- arrays
- literals
- operators
- arithmetic:
  - +, -, *, , %, ++, --
- assignment:
  - =, +=, -=, *=, /=, %=
- concatenation:
  - +
- relational:
  - ==, ===, !=, !==, >=, <=, <, <
- logical:
  - &&, ||, !
- keywords and statements
- common language constructs
- sequence
- selection:
  - ifelse
  - nested if
  - switch
- iteration:
  - pre-conditioned
  - post-conditioned
  - foreach mechanism
- JavaScript functions:
  - declarations:
    - name
    - parameters
    - code to be executed
    - return value
  - call and execution:
    - hoisting
    - self-invoking
  - third party libraries:
    - jQuery
- JavaScript objects:
  - objects:
    - including primitive data types:
      - numbers
      - Booleans
      - Strings
  - methods
  - properties
- JavaScript events:
  - common HTML events:
    - onblur
    - onchange

Teaching content:	
	▪ onclick ▪ onmouseover ▪ onmouseout ▪ onkeydown ▪ onload ▪ onsubmit ○ adding events to HTML elements: ▪ form elements ○ buttons ○ text box • JavaScript debugging: ○ debugging tools: ▪ built-in web browser: • Chrome developer tools • JavaScript console ○ third party: ▪ Firebug ○ exception handling: ▪ trythrowcatch block.
2.3	**Testing, debugging and threats**
Learners will be able to apply a range of testing and debugging techniques to ensure program accuracy and reliability, and evaluate common security threats and protection methods across websites, mobile platforms, and client-server environments	
2.3.1	Function of testing – compiling and debugging computer programs: • testing techniques: ○ black box vs white box testing ○ open and closed beta testing ○ workflow testing • selecting test data: ○ normal ○ extreme ○ invalid • code coverage: ○ percentage ○ logical pathways • bench run and test run • actual vs expected results • screen captures • remedial actions: ○ code modification ○ bug fixes • debug tools • watches • traces and step into • breakpoints • code inspection • trace tables • expected and actual results: ○ releases and versioning: • major/minor releases, patching, Concurrent Versioning System (CVS) ○ recording outcomes and recommendations:

Teaching content:	
	▪ known bugs, common vulnerabilities, and exposures (CVEs).

2.3.2	The considerations of security, threats and vulnerabilities to websites and mobile technology:
	
	• common client-side threats
	• current trends and attack vectors
	• current and classic examples:
	  ○ clickjacking
	• HTML injection and Cross-Site Scripting (XSS)
	• client-side cookies
	• password autocomplete
	• common server-side threats
	• current trends and attack vectors
	• current and classic examples:
	  ○ SQL injection
	  ○ directory traversal:
	  ▪ (“dot dot”, “” notation - downloading unauthorised files)
	  ○ source code reveal (bad server configuration)
	  ○ remote file inclusion (untrusted sources)
	  ○ client-side protection
	  ○ current and recommended techniques:
	  ▪ cache options:
	  • no cache
	  • no autocomplete
	  ○ client browser updates
	  ○ active cookie management
	  ○ First vs third party
	• server-side protection
	• current and recommended techniques:
	  ○ server configuration and patching for web server
	  ○ server side script engine and relational database
	  ○ secure sockets layer certification
	  • Hypertext Transfer Protocol (HTTP) only cookies
	  ○ web vulnerability scanner:
	  ▪ Acunetix
	  ○ awareness:
	  • Common Vulnerabilities and Exposures (CVE) list
	  ○ use of non-standard ports for services:
	  ▪ for relational database
	  ▪ web server
	  • File Transfer Protocol (FTP)
	  • Secure Shell (SSH) access
	• mobile platforms and applications
	• platforms types:
	  ○ commercial deployment platforms:
	  ▪ iOS: iPhone, iPad, iPod touch
	  ▪ Android
	• application types:
	  ○ native applications
	  ○ mobile web applications
	  ○ hybrid applications
	• types of reverse engineering:
	  ○ static analysis
	  ○ dynamic analysis
	• application hardening

Teaching content:	
	○ specific language issues ○ using improved coding technique: ▪ code obfuscation ▪ removal of debug code • improved exception handling.
2.4	**Design and create in programming**
Learners will be able to apply design principles and planning techniques to programming projects, using a range of tools and visual methods such as pseudocode, flowcharts, and structure diagrams. They will evaluate best practices in programming, project considerations, and user-centred approaches to ensure effective, inclusive, and goal-oriented development	
2.4.1	Applications of pseudocode: • readability • informality • expressiveness • modularity • algorithmic constructs • variables and data operations • comments • clarity and consistency.
2.4.2	The use of structure diagrams: • key terms and elements of a structure diagram: ○ sequence ○ selection ○ iteration • functional decomposition • when to use a structure diagram: ○ system design ○ module or component design ○ code refactoring ○ collaboration and communication ○ documentation • what a structure diagram describes: ○ components ○ relationships ○ hierarchical structure ○ interfaces and ports ○ packages and namespaces ○ multiplicity and cardinality.
2.4.3	Best practice in design and programming: • good programming principles: ○ avoid repetition of code ○ abstraction principle

Teaching content:	
	○ KISS – Keep It Simple Stupid! ○ avoid adding functionality until you need it ○ always opt for the simplest solution that will work ○ always make your code as easy to read and as understandable as possible ○ open/closed principle ○ always write code for the person who is going to maintain it ○ always follow standard conventions ○ single responsibility principle ○ minimise dependencies ○ avoid optimising until the code is working ○ reuse code where possible ○ familiarity with existing systems ○ separate different areas of functionality into distinct modules of code.
2.4.4	The applications of flow charts: • key terms and elements of a flowchart: ○ sequences of actions ○ inputs and outputs ○ processes ○ decisions ○ direction of flow ○ on/off page linkage • when to use flowcharts: ○ introduction to programming ○ program design and planning ○ algorithm development ○ problem solving ○ program documentation ○ system analysis.
2.4.5	A range of considerations in programming projects: • scope and requirements: ○ defining project goals, user needs, and key features ○ avoiding scope creep to keep projects manageable • technology selection: ○ choosing suitable programming languages, frameworks, and tools ○ ensuring compatibility, scalability, and long-term support • code quality and maintainability: ○ writing structured, well-documented, and reusable code ○ using version control to track changes • performance and efficiency: ○ optimising algorithms and resource usage for better speed • identifying bottlenecks through profiling and benchmarking • security and data protection: ○ implementing authentication, encryption, and secure coding practices ○ preventing vulnerabilities • testing and debugging: ○ applying unit, integration, and system testing ○ using debugging tools and error logging for issue resolution • collaboration and version control:

Teaching content:	
	○ working effectively in teams using repositories and branching strategies ○ maintaining clear and updated project documentation • deployment and scalability: ○ selecting appropriate hosting and cloud services ○ planning for increased user demand and system growth • user experience and accessibility: ○ designing intuitive, responsive, and accessible interfaces ○ ensuring compliance with accessibility standards • maintenance and future development: ○ planning for software updates, bug fixes, and new features ○ ensuring proper documentation for ongoing development.
2.4.6	A range of research methods: • experiments • surveys • data analysis • case studies • interviews • focus groups • literature reviews.
2.4.7	The application of real design tools in programming projects: • system architecture • Unified Modelling Language (UML) diagrams ○ flowcharts • user interface design ○ wireframing layouts • database structuring • Entity Relationship (ER) diagrams • algorithm and logic planning ○ pseudocode ○ state diagrams • collaboration and iteration ○ feedback ○ testing.
2.4.8	The application of planning techniques in programming projects: • project methodology: ○ Agile ○ Scrum ○ Waterfall • workflow mapping: ○ flowcharts ○ process diagrams • requirement analysis: ○ defining project scope and gathering user needs

Teaching content:	
	• task management: ○ timelines ○ version control.
2.4.9	The application of user-centred design principles: • user-centred design • functional and non-functional requirements • stakeholder engagement • ethics in software design • competitive analysis in software development • benchmarking existing digital solutions • inclusive programming practices • accessible UI/UX design • compliance with standards.
2.4.9	The importance of setting goals • sets clear values, objectives, and outcomes • defines purpose of a project • provides commitment to quality, functionality, and impact • economic contribution • motivates progress and accountability • motivates progress and accountability • guides resource allocation.
2.5	**System shell scripting**
Learners will be able to explore the features and practical applications of system shell scripting, using command-line tools to automate tasks, manage system configurations, and interact with files, processes, and network resources	
2.5.1	The key features and applications of operating system shell scripting: • common languages: ○ Sh, Bash (Linux) ○ PerlScript, Perl ○ MS Windows PowerShell ○ Windows Script Host (WSH) ○ MS Batch files ○ RubyScript, Ruby • command line interface (CLI): ○ MS Windows CMDexe, commandcom ○ Linux Terminal ○ OS X Mac Terminal • identification of shell script type by file extension • access to operating system • practical uses and scope: ○ automated tasks:

Teaching content:	
	▪ file maintenance ▪ installation ▪ batch jobs ○ configuration management: ▪ disks ▪ firewalls ▪ network connections ○ common commands: ▪ clearing screen ▪ using user-defined variables ▪ using environment variables ○ files: ▪ creating ▪ deleting ▪ renaming ▪ moving ▪ piping ○ folders/directories: ▪ change active ▪ creating ▪ deleting ▪ renaming ▪ moving ○ processes: ▪ start process ▪ kill process ○ branching: ▪ if statements ○ loops: ▪ for, while, do ○ screen output ○ keyboard input ○ mapping network folders ○ functions ○ library objects, methods, and properties ○ debugging.

Unit 2: Assessment Approach

The mode of assessment used for this unit is a Non-examination Assessment (NEA). This assessment method is externally set by TQUK and internally marked by centres.

The NEA for an individual unit cannot commence until the unit content has been fully taught to learners and TQUK mandatory standardisation training is completed.

An overview of the assessment approach is outlined in the table below:

Assessment description	The NEA comprises a brief designed to assess the learners' applied knowledge and skills and their ability to evidence critical analysis and reflective evaluation of the subject content.
Timings	The timeframe for the completion of the NEA is 10-12 hours
Assessment windows	The NEA brief is released in September each year. Centres have flexibility in scheduling the NEA within the academic session but must ensure it is completed by 30 April at the latest to allow for marking, internal quality assurance, and external moderation activities

The Non-examination Assessment will be conducted under controlled assessment conditions.

Centres **must** refer to the Assessment Guidance for the Delivery of Alternative Academic Qualifications document, available on our website, to ensure the appropriate administration and marking of this assessment and adherence to TQUK regulations.

The NEA has been carefully aligned with the assessment objectives (AOs) to create a consistent framework for learners. The table below confirms the assessment objectives that will be covered in the Non-examination Assessment.

Assessment objective	Description
AO4a – Research and plan	Learners are able to **research**, **investigate** and **plan** tasks, **choose** appropriate methods and actions.
AO4b - Review skills, methods and actions	Learners are able to **review** their skills, methods and actions
AO5- Demonstrate and apply skills and methods relevant to the given sector	Learners are able to **demonstrate** their application of technical skills relevant to the sector by **applying** the appropriate processes, tools and techniques

Unit 3: Cyber Security – Network Threats and Vulnerabilities

Unit Number:	R/651/5396		
Level:	3	**GLH:**	60
Unit Introduction:	This unit explores key cyber security concepts, focusing on network threats, vulnerabilities, and risk management. Learners will examine web application attacks, including injection attacks, authentication flaws, and Application Programming Interface (API) security, alongside tools for scanning and testing vulnerabilities. A critical aspect of cyber security is encryption and data protection. The unit introduces encryption algorithms, key management, and Secure Hashing (SHA) to protect data at rest and in transit. It also covers firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), proxy servers, and antivirus solutions, highlighting their role in securing networks. Learners will explore network and system configurations, including switch, domain, and antivirus settings, as well as best practices for web server security, access controls, and remote authentication. VPNand firewall configurations are examined to understand how secure communication is maintained. The unit also covers intrusion detection systems (Host-based Intrusion Dectection System (HIDS), Network-based Intrusion Detection System (NIDS), Intrusion Prevention System (IPS)) and their benefits, along with risk assessment strategies to mitigate vulnerabilities. Ethical considerations in cyber security, including privacy, regulatory compliance, and professional responsibility, are also addressed. Additionally, learners will investigate internal and external threats, such as malware, phishing, data breaches, and eavesdropping, as well as countermeasures like encryption, secure authentication, and network monitoring. Cyber attack methods, including session hijacking, SQL injection, and Denial-of-Service (DoS) attacks, are analysed to enhance security awareness. By the end of this unit, learners will have a strong foundation in cyber security principles, network defence mechanisms, and risk mitigation strategies.		
Assessment Type:	Examination Assessment (EA)		

Teaching content:	
3.1	**Cyber security basics**
Learners will be able to understand core principles of cyber security, including common web application vulnerabilities, encryption methods, protective software and hardware solutions, and key configuration practices to secure networks, systems, and data	
3.1.1	The properties of a web application attack suite: • web application scanning • vulnerability exploitation

Teaching content:	

	• input fuzzing
	• authentication and session management testing
	• reporting and documentation
	• areas of testing:
	  ○ injection attacks:
	  ○ Cross-Site Scripting (XSS)
	  ○ Cross-Site Request Forgery (CSRF)
	  ○ security misconfigurations
	  ○ authentication and authorisations
	  ○ information leakage
	  ○ business logic flaws
	  ○ file upload vulnerabilities
	  ○ API Security
	  ○ secure communications
	  ○ compromised credentials:
	  ▪ missing/misconfigured encryption
	  • trust relationships:
	  ▪ compromised cached credentials.

3.1.2	A range of data encryption terminology in network security testing:
	
	• confidentiality:
	  ○ ensuring that data is only accessible to authorised users and remains private
	• secure communication:
	  ○ transmitting data over a network in a way that prevents interception or tampering
	• data-at-rest protection:
	  ○ applying security measures to data stored on physical or digital media to prevent unauthorised access
	• encryption in-flight:
	  ○ protecting data while it is being transmitted across a network to prevent interception
	• encryption-at-rest:
	  ○ encrypting stored data to safeguard it from unauthorised access even if the storage medium is compromised
	• encryption algorithms and strength:
	  ○ mathematical formulas used to encrypt and decrypt data, with strength determined by key length and complexity
	• key management:
	  ○ securely generating, storing, distributing, and disposing of encryption keys to prevent unauthorised access
	• secure hashing algorithm (SHA):
	  ○ cryptographic hashing function that converts data into a fixed-length hash to ensure data integrity
	• key exchange methods:
	  ○ secure techniques for exchanging cryptographic keys between communicating parties
	  ○ Diffie-Hellman: method for securely exchanging cryptographic keys over a public channel without prior shared secrets
	• compliance requirements:
	  ○ regulatory and industry standards that govern the use of encryption and data protection measures
	• performance impact:
	  ○ the effect of encryption on system speed, resource consumption, and overall efficiency

Teaching content:	

	• Secure Sockets Layer (SSL) inspection:
	  ○ decrypting and analysing encrypted SSL/ Transport Layer Security (TLS) traffic to detect security threats and enforce policies
	• encryption auditing and testing:
	  ○ evaluating encryption implementations through testing and assessments to ensure security and compliance.

3.1.3	The properties of a range of software and hardware solutions:
	
	• firewalls:
	  ○ software-based and dedicated hardware
	  ○ firewall as a service (FWaaS)
	• proxy server
	• Firewall Layer 7 inspection capability
	• intrusion detection system
	  ○ NIDS
	  ○ HIDS
	  ○ IPS
	  ○ EDR
	  ○ XDR
	• network-based antivirus
	• internet content filter:
	  ○ URL filtering
	  ○ keyword filtering
	  ○ category filtering
	  ○ content scanning
	  ○ time-based filtering
	  ○ HTTPS filtering
	  ○ reporting and logging
	  ○ SSL inspection
	• spam filter:
	  ○ Deny List
	  ○ Allow List.

3.1.4	Types of configuration and their purpose:
	
	• switch configuration:
	  ○ implementing Virtual Local Area Networks (VLANs)
	  ○ protection from loops:
	  ▪ using Spanning
	  ○ using Spanning Tree Protocol
	  ○ Sticky MAC
	  ○ ports not active by defaults, only active if device is connected
	• antivirus configuration:
	  ○ frequency of virus signature updates
	  ○ 'on demand' scanning settings for downloads and email attachments
	  ○ scanning frequency
	  ○ integration with operating systems and email systems
	  ○ tamper protection with a strong password
	  ○ anti-virus logging to a log collector
	  ○ restriction of USB/optical media
	• domain configuration:
	  ○ authentication of users
	  ○ authorisation of users

Teaching content:	
	○ user permissions and default behaviour ○ creation, maintenance and application of group security policies ○ bandwidth throttling ○ roaming user profiles and desktops ○ Remote Desktop Services (RDS) ○ Remote Desktop Protocol (RDP) ○ user groups • web technology security and configuration • awareness of: ○ Windows, Apache, MySQL, PHP (WAMP) ○ Linus, Apache, MySQL, PHP (LAMP) ○ Mac, Apache, MySQL, PHP MAMP stacks • web server configuration: ○ suppressing web server footprint: ▪ name ▪ version ▪ disable built-in accounts • aliases and virtual hosts • ports for HTTP/HTTPS traffic: ○ 80, 443, 8080 etc • automatic HTTP to HTTPS redirects • session timeout constraints • allowed/blocked IP ranges • suppressing directory views • directory/folder permissions • file permissions • file type execution: ○ ASP Net, ASP, PHP • suppressing web application code errors • limit maximum concurrent connections • File Transfer Protocol (FTP) (client) access: ○ allowed/blocked IP ranges ○ use of FTPS (also known as FTP-ES, FTP-SSL and FTP Secure) • SSH remote access • relational database remote access and authorisation: ○ allowed/blocked IP ranges ○ non-standard ports ○ disable standard accounts ○ change default passwords ○ user permissions, especially for Data Definition Language (DDL).
3.2	**Security technologies**
Learners will be able to evaluate the features and benefits of key network security technologies, including intrusion detection and prevention systems, VPNs and tunnelling protocols, and firewall configurations used to protect systems against unauthorised access and cyber threats	
3.2.1	The features and benefits of types of intrusion detection systems: • HIDS features ▪ host-based monitoring ▪ intrusion detection ○ benefits

Teaching content:	
	▪ host-level visibility ▪ early threat detection ▪ malware detection • IPS: ○ features ▪ traffic monitoring ▪ intrusion detection ▪ threat prevention ○ benefits ▪ threat prevention ▪ real-time protection ▪ enhanced security posture • NIDS: ○ features ▪ real-time monitoring ▪ intrusion detection ▪ traffic analysis ○ benefits ▪ early threat detection ▪ enhanced security posture.
3.2.2	The properties of VPN and tunnelling protocols: • virtual private networks • open-source VPN • tunnelling protocols • encryption (AES 256) • Diffie-Hellman • Secure Hashtag Algorithm (SHA).
3.2.3	The features of firewall configuration: • commercial and open source solutions • bespoke hardware firewalls • FWaas • active threat management • Network Address Translators (NATs) • deny list, allow list • blocking by: ○ protocol ○ port ○ IP address (source or destination) ○ MAC address (source or destination) ○ URL if the firewall has Layer 7.
3.3	**Managing risks, threats, and vulnerabilities in cyber Security**
Learners will be able to assess the impact of internal and external cyber security threats, explore preventative technologies and configuration practices, and apply risk management strategies to protect systems, networks, and data from malicious attacks and vulnerabilities	
3.3.1	The stages in planning and managing risks and vulnerabilities: • regulations • procedure

Teaching content:	
	• baseline • guideline • layering • education • backup and recovery strategies • upgrading • setting up file and folder permission • vulnerability scanning • vulnerability management solution • root cause analysis • risk assessment • remediation: ○ remediation report.

3.3.2	The influence of ethical responsibilities on cyber security practice:
	
	• assurance of:
	  ○ reliability
	  ○ accuracy
	  ○ availability
	  ○ safety
	  ○ security
	• continuing professional development (CPD)
	• awareness of alerts and advisories:
	  ○ Microsoft
	  ○ Open Web Application Security Project (OWASP)
	  ○ Certified Information Systems Security Professional (CISSP)
	  ○ open source
	  ○ CVE
	• balance of individual privacy and security needs
	• membership of professional bodies,
	  ○ information systems security association (ISSA).

3.3.3	Considerations of external threats and security vulnerabilities:
	
	• malware and its features:
	  ○ Virus
	  ○ Spyware
	  ○ Adware
	  ○ Back doors
	  ○ Polymorphic
	  ○ Trojan
	  ○ Worm
	  ○ Ransomware
	  ○ CryptoLocker
	  ○ Bots
	  ○ Rootkits.
	
	• exploits:
	  ○ client side
	  ○ server side
	  ○ scanner
	  ○ module
	  ○ payload
	  ○ trigger

Teaching content:	
	○ injection ○ pivoting ○ spoof ○ shell code ○ vulnerability when weaponised into an exploit.
3.3.4	The influence of inadequate security practice on cyber security management: • Web server attack vectors: ○ source code reveal (bad server configuration) non-patching of flawed code ○ poor session management: ▪ no timeout ▪ invalidation ○ broken authentication: ▪ sessionID reveal in URL ○ poor security management: ▪ use of unpatched, out of date and vulnerable frameworks which are exposed ▪ unsecured data in motion: ▪ no use of SSL ○ poor management of folders/directories ○ poorly configured virtual hosts and aliases ○ unsecured cookies ○ footprint reveal of web server-based technologies: ▪ server side scripting languages supported ▪ version information ▪ server environment variables ○ Web application attack vectors- client-side techniques: ▪ clickjacking • HTML injection and Cross-site scripting • not disabling built-in accounts • not changing default passwords.
3.3.5	The effect of a range of internal threats and vulnerabilities: • unauthorised access: ○ accidental damage: ▪ localised disasters: • fire • water leak ○ human error ○ technical error ○ equipment failure or damage ○ theft or loss of data ○ unauthorised modification of data ○ shoulder surfing ○ accidental disclosure or deletion ○ phishing ○ vishing ○ smishing ○ data breach: ▪ sending files to personal email account ○ actions of disgruntled employees: ▪ intentional disclosure or deletion ▪ malicious damage

Teaching content:	
	▪ industrial espionage • carelessness: ▪ sensitive data on portable devices ▪ lost/stolen devices ▪ connecting to insecure networks.
3.3.6	The origin and effects of eavesdropping and open network: • eavesdropping can happen through: ○ Network Sniffing ○ Man-in-the-Middle (MitM) Attacks ○ wireless eavesdropping ○ pickup devices for sound and video: ▪ smart speakers • eavesdropping consequences: ○ disclosure of sensitive information ○ data tampering or manipulation ○ data leakage ○ reputational damage ○ potential regulatory financial penalties • open network threats can occur through: ○ MitM Attacks ○ network sniffing ○ malware distribution ○ data interception ○ rogue access points ○ DoS Attacks ○ session hijacking ○ unauthorised devices: ▪ wireless Keyboard, video and mouse (KVM).
3.3.7	The methods of mitigating risk of eavesdropping and open network attacks: • mitigating risk of eavesdropping: ○ encryption ○ secure network design ○ use of secure protocols ○ wireless security ○ regular updates and patches ○ authentication ○ network monitoring ○ network access control • mitigating risk of open network threats: ○ use secure connections ○ avoid sharing sensitive information ○ enable firewall and antivirus protection ○ be wary of rogue networks ○ disable auto-connect ○ keep software updated ○ use two-factor authentication (2fa) ○ intrusion detection/intrusion protection devices: ▪ network access control to detect suspicious traffic: • command and control.
3.3.8	The components and terminology of cyber attacks:

Teaching content:	

	• WPA3
	• WPA-TKIP
	• session hijacking
	• flash cookies
	• cookies and attachments
	• compromised key attack
	• password attack
	• network sniffing
	• application layer attack
	• Identity spoofing (IP address spoofing)
	• URL hijacking
	• client-side attacks
	• amplification attack
	  ○ smurf
	  ○ fraggle
	• SYN flood
	• SQL injection attack
	• bluesnarfing
	• rogue access point
	• snorting or sniffing
	• Domain Name System (DNS) spoofing
	• Media Access Control (MAC) spoofing.

3.3.9	The application of security settings to network technologies:
	
	• digital certification
	• types of certificate:
	  ○ self-signed
	  ○ CA-issued
	  ○ different vendor classes
	• contents of a digital certificate
	• deployment of a certificate management solution
	• public key infrastructure (PKI)
	• certificate authority (CA)
	• creating self-signed certificates
	• deploying keys and certificates
	• operating system management:
	  ○ windows active directory certificate services
	  ○ Windows 11 onwards required a trusted platform model
	  ○ Mac OS X Keychain.

3.3.10	The different forms of network defence: • vVPN • subnets • VLANs • private local area networks (PVLANs) • Network Access Control (NAC) • IPS • IDS • Breach and Attack Simulation (BAS).
3.3.11	The effects of configuration and hardening:

Teaching content:	
	• session timeout periods • change default passwords • static vs dynamic IP addresses • non-broadcast of Service set Identifer (SSID) • use of non-standard ports for network services • quality of service (QoS) • logging access and activity • multifactor authentication • only opening required IP/UDP ports.

3.3.12	The features of XSS:
	
	• stored
	• reflected
	• redirected attacks
	• document object model (DOM) based XSS
	• client side cookies
	• password autocomplete
	• cross-site request forgery (CSRF)
	• web application attack vectors- server side techniques:
	  ○ SQL injection
	  ○ lack of bound variables
	  ○ no stored procedures
	• directory traversal
	• remote file inclusion
	• session hijacking (fixation)
	• insecure direct object references.

Unit 3: Assessment Approach

The mode of assessment used for this unit is an Examination Assessment (EA). This assessment method is externally set and marked by TQUK, ensuring consistency and reliability in the evaluation of learner's knowledge and understanding.

An overview of the assessment approach is outlined in the table below:

Assessment description	The EA comprises a balance of multiple-choice questions (MCQ), extended-response questions (ERQ) and short-answer questions (SAQ).
Assessment windows	Late January/early February** and early May Centres have the flexibility to timetable the Examination Assessment within the specified assessment window.
Duration of EA	1 hour 30 minutes

** **Important**: in the first year of delivery, there is no assessment window opportunity in January 2027. Thereafter, EAs will be available annually in late January/early February and mid-May.

The Examination Assessment will be conducted under exam conditions in a controlled environment. Centres must refer to the Assessment Guidance for the Delivery of Alternative Academic Qualifications document available on our website for further information to support the administration of the EA.

The assessment has been carefully aligned with the unit's assessment objectives (AOs) to create a consistent framework for learners. The table below confirms the assessment objectives that will be covered in the Examination Assessment.

Assessment objective	Description
AO1 – Recall knowledge and information	Learners are to **recall** knowledge and information
AO2 – Apply knowledge and information	Learners are to **apply** knowledge and information to situations and contexts relevant to the given sector
AO3 – Interpret, analyse or evaluate information, ideas or different viewpoints	Learners are able to **interpret**, **analyse** or **evaluate** information, ideas or different viewpoints to make judgements that are reasoned or draw conclusions.

Unit 4: Network Security Management and Data Gathering - Technical Support

Unit Number:	T/651/5397		
Level:	3	**GLH:**	60
Unit Introduction:	This unit provides learners with an in-depth understanding of network security legislation, technical security measures, and data gathering techniques, equipping them with the knowledge and skills necessary to support and maintain secure networks. The unit begins with an exploration of legislation in network security management, focusing on key laws such as the Computer Misuse Act (1990), the Data Protection Act (1998), and the General Data Protection Regulation (GDPR, 2018). Next, learners will explore security management, covering both hardware and software solutions for securing networks. This includes firewalls, intrusion detection systems (IDS/IPS), encryption protocols, access control mechanisms, and authentication methods such as biometrics and digital signatures. Additionally, learners will gain insights into network security maintenance, learning how organisations monitor and respond to security threats using log analysis, vulnerability scanners, and Security Information and Event Management (SIEM) tools. The unit will also introduce key network policies, such as VPN implementation, password security, and remote access guidelines, alongside the role of Service Level Agreements (SLAs) in maintaining security standards. Learners will examine different data collection techniques, including surveys, observations, and real-world measurements, and explore statistical concepts such as mean, median, variance, and data distribution. The unit also introduces probability and recursion, focusing on their applications in cybersecurity, such as binary search, quicksort, and directory traversal algorithms.		
Assessment Type:	Non-Examination Assessment (NEA)		

Teaching content:	
4.1	**Legislation in network security management**
Learners will be able to understand the application of key legislation related to network security and best practices, and evaluate the consequences of non-compliance through real-world case studies, including their impact on individuals, organisations, and data governance	
4.1.1	The application of current legislation for network security best practice: • Computer Misuse Act (1990) • Data Protection Act (1998) • General Data Protection Regulation (2018).

4.1.2	The consequences of violation of current legislation for security network best practice
	
	• Computer Misuse Act (1990):
	  ○ Gary McKinnon (2001-2002)
	  ○ TalkTalk Cyber Attack

Teaching content:	

	• Data Protection Act (1998):
	  ○ T-Mobile Data Breach (2009)
	  ○ Sony Playstation Network Hack (2011)
	• General Data Protection Regulation (2018):
	  ○ British Airways Data Breach (2018)
	  ○ Facebook-Cambridge Analytica Scandal (2018).

4.2	**Security management**
Learners will be able to apply principles of hardware, software, and cryptographic security, and understand how continuous network security monitoring and security policies contribute to maintaining system integrity, mitigating risks, and ensuring ongoing compliance	

4.2.1	The application of hardware and software for network security:
	
	• intrusion detection and prevention systems:
	  ○ firewalls
	  ○ virus protection
	  ○ spyware protection
	  ○ file and folder monitoring
	  ○ alarms
	  ○ honeypots
	  ○ IPS
	  ○ IDS
	  ○ NAC
	• cryptography algorithms and protocols:
	  ○ encryption:
	  ▪ symmetric encryption
	  ▪ asymmetric encryption
	  ▪ data integrity algorithms
	  ▪ authentication protocols
	• access control
	• biometrics
	• passwords
	• user permissions
	• digital signatures
	• protocols
	• logins:
	  ○ Privilege Access Management (PAM)
	• WPA3
	• Temporal Key Integrity Protocol TKIP
	• MAC association
	• email security features
	• spam filters
	• email encryption
	• attachment scanners
	• email scanners.

4.2.2	The application of network security maintenance principles:
	
	• different phases of Continuous network security monitoring (CNSM) :
	  ○ plan:
	  ▪ discover
	  ▪ classify
	  ▪ define policies

Teaching content:	
	▪ apply security measures ▪ monitor ▪ analyse ▪ collect/aggregate ○ action: ▪ escalate ▪ validate ○ logs: ▪ event ▪ audit ▪ security ▪ access ○ tools: ▪ banner grabbing ▪ vulnerability scanner ▪ honeypots ▪ honeynets ▪ passive vs active tolls ▪ port scanner ▪ protocol analyser ▪ Security Information Events Management (SIEM) ○ types of network policies: ▪ VPN ▪ password ▪ audit - network and system components ▪ acceptable encryption ▪ information sensitivity ▪ antivirus guidelines ▪ wireless communications ▪ risk assessment ▪ Expanded Memory Specification (EMS) network and computer acceptable use ▪ remote access ▪ acceptable use ▪ automatically forwarded email ○ role and purpose of SLAs ▪ services, priorities and responsibilities ▪ information-gathering, analysing, documenting, educating, negotiating, consensus-building ▪ measuring performance and quality ▪ log review ▪ instruction detection.
4.3	**Data gathering**
Learners will be able to apply a range of methods for gathering, interpreting, and analysing data, and use statistical and algorithmic strategies such as probability, sequences, and recursion to identify patterns, support informed decision-making, and solve complex computing problems	
4.3.1	The methods of data gathering: • representing data

Teaching content:	
	○ concepts and techniques for comparing data sets: ▪ range and range limits ▪ averages: arithmetic mean, median (middle value), mode (most frequent) ▪ relationship between mean, median, mode ▪ distribution, positive or negative skew ▪ variance ▪ histograms • gathering data: ○ primary and secondary data ○ quantitative and qualitative data ○ common methods of gathering data: ▪ real world measurements ▪ observation ▪ questionnaires ▪ surveys ○ extraction of required information from raw data ○ limitations of data gathered ▪ accuracy ▪ sample size ▪ need for cleaning invalid data points • interpreting data • analysing summary data • identification of trends and recurring patterns • proving a hypothesis.
4.3.2	Strategies for calculating with sequences, series, probability and recursion: • probability: ○ probability terminology and usage: ▪ probability definition ▪ probability line ▪ experiment or trial ▪ sample space and sample point ▪ events and event types (dependent, independent, mutually exclusive) ○ space diagrams: ▪ double' values when two dice are thrown • visualising events: ○ venn diagrams ▪ mutually exclusive vs. non-mutually exclusive events ○ tree diagrams ▪ dependent vs. independent events • recursion: ○ series: ▪ Fibonacci ▪ Factorial ○ rules of recursion: ▪ have a base case ▪ state change toward base case ▪ must call itself ○ common recursive algorithms used in computing: ▪ factorial ▪ quicksort ▪ binary search ▪ directory traversal ▪ Sierpinski triangle.

Go to contents Page >

Unit 4: Assessment Approach

The mode of assessment used for this unit is a Non-examination Assessment (NEA). This assessment method is externally set by TQUK and internally marked by centres.

The NEA for an individual unit cannot commence until the unit content has been fully taught to learners and TQUK mandatory standardisation training is completed.

An overview of the assessment approach is outlined in the table below:

Assessment description	The NEA comprises a brief designed to assess the learners' applied knowledge and skills and their ability to evidence critical analysis and reflective evaluation of the subject content.
Timings	The timeframe for the completion of the NEA is 9-11 hours
Assessment windows	The NEA brief is released in September each year. Centres have the flexibility in scheduling the NEA within the academic session but must ensure it is completed by 30 April at the latest to allow for marking, internal quality assurance, and external moderation activities

The Non-examination Assessment will be conducted under controlled assessment conditions.

Centres **must** refer to the Assessment Guidance for the Delivery of Alternative Academic Qualifications document, available on our website, to ensure the appropriate administration and marking of this assessment and adherence to TQUK regulations.

The NEA has been carefully aligned with the assessment objectives (AOs) to create a consistent framework for learners. The table below confirms the assessment objectives that will be covered in the Non-examination Assessment.

Assessment objective	Description
AO4a – Research and plan	Learners are able to **research**, **investigate** and **plan** tasks, **choose** appropriate methods and actions.
AO4b - Review skills, methods and actions	Learners are able to **review** their skills, methods and actions
AO5- Demonstrate and apply skills and methods relevant to the given sector	Learners are able to **demonstrate** their application of technical skills relevant to the sector by **applying** the appropriate processes, tools and techniques.

Unit 5: Website Technology – Scripting and Programming

Unit Number:	Y/651/5398		
Level:	3	**GLH:**	60
Unit Introduction:	This unit introduces the essential technologies and tools used to build websites. Learners will explore the hardware and software needed for web development, including web servers, databases, computers, and mobile devices. They will also learn about browsers, file transfer tools, and website-building software like Dreamweaver and Notepad++. A key focus is on how websites work, including the languages and standards used to create them. Learners will understand how HTML structures content, CSS controls design, and JavaScript adds interactivity. They will also explore server-side languages like PHP and ASP.NET, which help websites process information. The unit covers how to style websites using CSS, including colours, fonts, layouts, and spacing. Learners will also understand how different browsers display websites and how to ensure consistency. Finally, the unit explains HTML basics, including how to format text, create links, add images, and build simple forms. Learners will practice writing clean, well-structured code to create user-friendly websites. By the end of this unit, learners will have a solid understanding of how websites are built and styled, preparing them for more advanced web development.		
Assessment Type:	Non-Examination Assessment (NEA)		

Teaching content:	
5.1	**Website technology**
Learners will be able to explore the hardware, software, and protocols that underpin website technologies, and understand how web standards, scripting languages, and formatting techniques are applied to ensure compatibility, functionality, and accessibility across platforms and devices	

5.1.1	The characteristics of hardware and software used in website technology:
	
	• hardware:
	  ○ server-side
	  ○ web server
	  ○ relational database server
	  ○ client-side
	  ○ desktop:
	  ▪ PC
	  ▪ Apple Mac
	  ○ mobile device:
	  ▪ smart phone
	  ▪ tablet
	• software application:
	  ○ server-side
	  ▪ web server:
	  • Apache HTTP

Teaching content:	
	• Microsoft ○ internet information services (IIS): ▪ Nginx ▪ Google GWS ○ relational database system: ▪ MSSQL ▪ SQL ▪ Oracle Database ▪ PostgreSQL ▪ IBM Db2 ▪ SQLite ▪ MariaDB ○ client-side ▪ web browser: • Internet Explorer (IE) • Google Chrome • Mozilla Firefox • Apple Safari ○ FTP client: ▪ Filezilla ○ secure shell client: ▪ PuTTY ○ text editors: ▪ Notepad++ ○ web development (What you see is what you get (WYSIWYG)) tools: ▪ Adobe Dreamweaver ○ Pre-packaged bundles: ▪ LAMP ▪ WAMP ▪ MAMP ○ Protocols and ports: ▪ file transfer protocol (FTP), port 21 ▪ secure shell (SSH), port 22 ▪ HTTP, port 80 ▪ SSL, port 443.
5.1.2	The application of website technologies and standards: • separation of content from formatting: ○ markup languages: ▪ HTML ○ style sheet languages: ▪ CSS ○ client-side scripting languages: ▪ JavaScript ○ server-side scripting: ▪ PHP hypertext pre-processor (PHP) ▪ active server pages (ASPnet) ▪ Java server pages (JSP) ○ third party libraries: ▪ jQuery ○ data description methods: ▪ XML (eXtensible Markup Language) ▪ JSON (JavaScript Object Notation) ○ website standards

Teaching content:	
	○ World Wide Web Consortium (W3C) ○ HTML 5 ○ CSS 2 and 3 ○ JavaScript ○ markup validation service for: ▪ HTML ▪ CSS ○ client compliance and testing: ▪ web browser HTML5 test ▪ Acid3.
5.2	**Scripting and programming language**
Learners will be able to apply style sheet and markup languages to develop well-structured, visually effective web content, demonstrating understanding of syntax, formatting rules, layout control, and accessibility considerations across a range of browsers and devices	
5.2.1	The application of style sheet language: • CSS 3: ○ web browser support (browser and version) ○ cross-browser differences ○ CSS elements and syntax: ▪ purpose (format and layout) ○ selectors: ▪ types (element, id, class) ▪ grouping ○ declaration: ▪ property ▪ value pairs ○ hyperlinks: ▪ pseudo classes and elements: ▪ <a> link ▪ visited ▪ active ▪ hover ▪ before, after ○ cross-browser issues: ▪ rendering variances • CSS units: ○ measurement values: ▪ %, in (inch) ▪ cm (centimetre) ▪ mm (millimetre) ▪ em ▪ ex ▪ pt (point) ▪ pc (pica) ▪ px (pixels) • CSS box model: ▪ content ▪ padding ▪ border ▪ margin ▪ effect on height and width of content

Teaching content:	
	• CSS insertion methods: ▪ external style sheet <link> ▪ internal style sheet <style></style> ▪ inline styles ▪ inheritance priority from multiple style sheets • CSS common properties: ▪ background ▪ border ▪ colour ▪ height ▪ margin ▪ padding ▪ text-align ▪ width ▪ combination of common properties to produce visual themes ▪ circumstances when alternate visual themes are necessary: • high contrast for visually impaired users • CSS colors (the American spelling of colour is used for CSS) ○ color value formats: ▪ Hexadecimal ▪ Red Green Blue (RGB) ▪ Red Green Blue Alpha channel (RGBA) ▪ Colour names.
5.2.2	The application of markup language: • HTML elements and syntax: ○ purpose (content) ○ tags, nested tags ○ tag attributes ○ DOCTYPES (standards): ▪ HTML 401 transitional or strict ▪ XHTML11 ▪ HTML5 ○ case sensitivity ○ HTML page structure: ▪ <html></head> HTML document ▪ <head></head> HTML title ▪ meta tags: keywords, description, author, refresh ▪ <body></body> HTML body • HTML basic tags: ○ structure and text tags: ▪ Paragraph ▪ <h></h> Headline ▪ <pre></pre> Pre-formatted text ▪ Horizontal rule ○ hyperlinks: ▪ links <a>: ▪ hyperlink to another resource (page or domain) ▪ image link ▪ mailto link ▪ same page target ▪ same page hyperlink ○ lists: ▪ ordered

Teaching content:	
	▪ ▪ unordered items ○ IDE Templates ○ Form name and ID attributes.

Unit 5: Assessment Approach

The mode of assessment used for this unit is a Non-examination Assessment (NEA). This assessment method is externally set by TQUK and internally marked by centres.

The NEA for an individual unit cannot commence until the unit content has been fully taught to learners and TQUK mandatory standardisation training is completed.

An overview of the assessment approach is outlined in the table below:

Assessment description	The NEA comprises a brief designed to assess the learners' applied knowledge and skills and their ability to evidence critical analysis and reflective evaluation of the subject content.
Timings	The timeframe for the completion of the NEA is 9-11 hours
Assessment windows	The NEA brief is released in September each year. Centres have the flexibility in scheduling the NEA within the academic session but must ensure it is completed by 30 April at the latest to allow for marking, internal quality assurance, and external moderation activities

The Non-examination Assessment will be conducted under controlled assessment conditions.

Centres must refer to the Assessment Guidance for the Delivery of Alternative Academic Qualifications document, available on our website, to ensure the appropriate administration and marking of this assessment and adherence to TQUK regulations.

The NEA has been carefully aligned with the assessment objectives (AOs) to create a consistent framework for learners. The table below confirms the assessment objectives that will be covered in the Non-examination Assessment.

Assessment objective	Description
AO4a – Research and plan	Learners are able to **research**, **investigate** and **plan** tasks, **choose** appropriate methods and actions.
AO4b - Review skills, methods and actions	Learners are able to **review** their skills, methods and actions
AO5- Demonstrate and apply skills and methods relevant to the given sector	Learners are able to **demonstrate** their application of technical skills relevant to the sector by **applying** the appropriate processes, tools and techniques

Section 3: Assessment and Achievement

Assessment Objectives and Weightings

The assessment objectives for the qualification are set out below and provide the basis for the assessment of each unit.

- AO1, AO2, and AO3 are assessed through Examination Assessments (EAs)
- AO4 and AO5 are assessed through Non-Examination Assessments (NEAs).

The following table outlines the overall weightings of each assessment objective across the qualification.

	Assessment Objective	Weighting
EA	AO1 Recall knowledge and information Learners are able to recall knowledge and information.	4%
	AO2 Apply knowledge and information Learners are able to apply knowledge and information to questions, problems, or scenarios.	18%
	AO3 Interpret, analyse or evaluate information, ideas or different viewpoints Learners are able to interpret, analyse or evaluate information, ideas, or different viewpoints to make judgements that are reasoned or draw conclusions.	18%
NEA	AO4a Research and plan AO4b Review skills, methods and actions Learners are able to research, investigate, and plan tasks, choose appropriate methods and actions as well as review these skills, methods, and actions.	26%
	AO5 Demonstrate and apply skills and methods relevant to the given sector Learners are able to demonstrate their application of technical skills relevant to the sector by applying the appropriate processes, tools, and techniques.	34%

In Examination Assessments, the primary focus is on applying knowledge, interpreting, and analysing information.

In non-examination assessments, the weighting is more balanced between research, planning, review, and the demonstration of sector-relevant skills and methods.

This table details how marks are allocated across the assessment objective in each assessment.

	AO1	AO2	AO3	AO4a	AO4b	AO5
Unit 1	11%	45%	44%			
Unit 2				33%	11%	56%
Unit 3	10%	42%	48%			
Unit 4				43%		57%
Unit 5				43%		57%

Assessment Adaptation

Centre adaptation of the Examination Assessment or Non-examination Assessment is **not permitted**. This is to ensure that the qualification as a whole, and each associated assessment task, retains its reliability and comparability across centres and learners. TQUK has taken the approach of externally setting the assessments to ensure that each learner has a fair opportunity to achieve the qualification.

Grading and Marking

Grading and Aggregation

The grading structure for the qualification comprises Pass, Merit, and Distinction for the component assessments and Pass, Merit, Distinction, and Distinction* for the overall qualification grade.

TQUK will use a Uniform Mark Scheme (UMS) to aggregate grades. The standard for a pass will be decided by a minimum mark which is correlated to a UMS. The UMS will be able to factor in variations across unit achievement and over time to ensure comparability across mark ranges and assessment series.

Each assessment will be marked against the raw marks and at the awarding meeting, cut scores for each of grade boundaries for pass, merit and distinction will be decided. These will then be converted into the UMS for that unit. The UMS for each unit will then be aggregated into a qualification grade.

The qualification follows a compensatory grading model, meaning that marks from different assessments are aggregated. Learners do not need to achieve a minimum mark in individual units, as the final qualification grade is based on the total UMS marks gained across all assessments.

Each unit assessment contributes a set percentage to the final qualification grade. The total UMS score for the qualification is 500 marks, with assessments weighting and marks as follows:

Unit	Assessment method	Weighting	Raw marks	UMS marks
Unit 1	EA 90GLH	24%	75	120
Unit 2	NEA 90GLH	24%	72	120
Unit 3	EA 60GLH	16%	50	80
Unit 4	NEA 60GLH	18%	56	90
Unit 5	NEA 60GLH	18%	56	90
			309	500

The overall percentage grading scale for each unit is:

Grade	%
Not Yet Achieved	0-39%
Pass	40-59%
Merit	60-79%
Distinction	80-100%

Grade boundaries

The grade boundaries for the UMS for each unit are as follows:

Unit	Pass	Merit	Distinction
Unit 1	48	72	96
Unit 2	48	72	96
Unit 3	32	48	64
Unit 4	36	54	72
Unit 5	36	54	72

Learners' final grades for the qualification are determined using the following UMS boundaries:

Grade	Boundary
Not Yet Achieved	0-199
Pass	200-299
Merit	300-399
Distinction	400-449
Distinction*	450-500

The grade of Distinction* will be awarded at **qualification level** to learners scoring marks of 450 and above overall.

Aggregation for the award of the qualification will be based on the sum of marks awarded for the UMS across all the units and awards will be made in line with the qualification grade thresholds. There will be no minimum expectation within units as the qualification is fully compensatory.

These UMS grade boundaries ensure consistency across assessment series while allowing for adjustments in raw mark thresholds, which are finalised in the awarding meeting.

A grading calculator is available to support centres in calculating final grades. This can be downloaded from Verve/the TQUK management system.

Marking approach

The qualification follows a structured marking approach designed to ensure that learners are assessed consistently across all qualification outcomes. This approach rewards learners for demonstrating their knowledge, understanding, and skills, providing a fair and reliable indication of their achievement.

The marking system allows for full compensation, meaning that there is no minimum threshold of achievement required within individual assessments. Learners can demonstrate a broad range of knowledge and skills across the qualification, making their final grade a meaningful indicator of ability for higher education institutions and employers.

This approach also supports assessors in differentiating between different levels of performance within units. It provides a detailed and accurate measure of learner achievement while balancing positive and negative variations in assessment performance, ensuring that the final aggregated mark reflects a learner's overall ability.

Examination Assessments are marked using a combination of points-based and levels-based mark schemes, depending on the type of question and level of demand. For example:

- multiple-choice questions (MCQs) are marked using a points-based system.
- short-answer questions (SAQs) and extended response questions (ERQs) are marked using a levels-based approach.

The examination paper is designed to align with the assessment objective weightings, ensuring that knowledge recall, application, and evaluation skills are measured appropriately.

Non-examination Assessments are marked using a levels-based approach with four distinct mark bands. This structure provides a clear and consistent way for assessors to differentiate between levels of performance. The four-band system helps prevent grades clustering at the Merit level (known as 'regression to the mean') and instead ensures that learners are more reliably placed within the grading structure of Pass, Merit, or Distinction. Please refer to the Assessment Guidance for the Delivery of the Alternative Academic Qualifications for full marking guidance.

Once raw marks have been assigned, they are converted into the Uniform Mark Scheme (UMS), ensuring that final grades remain fair and comparable across different assessment series.

This marking approach ensures that all assessments provide a robust, valid, and fair measure of learner performance, supporting progression to further study or employment.

Awarding Meeting and Grade Boundary Setting

TQUK will hold an awarding meeting following each assessment session to determine grade boundaries for the qualification. The awarding meeting is a critical part of the quality assurance process, ensuring that results are fair, reliable, and comparable across different assessment sessions.

During the judgemental review, the committee will independently review learner work for all units at Pass, Merit, and Distinction, focusing on mark ranges identified within each grade boundary.

While the grading scale and UMS boundaries have been pre-set, the actual raw mark cut scores for each grade may vary from series to series based on assessment difficulty.

The awarding meeting will use statistical analysis and expert judgement to review learner performance. If an assessment is found to be more or less challenging than expected, the raw mark boundaries may be adjusted to ensure fairness and consistency.

Once awarding activities, including internal scrutiny, are completed, TQUK will:

- convert raw marks to UMS marks for each unit.
- apply unit grades based on UMS scores.
- determine the final qualification grade for each learner based on their aggregated UMS score.

TQUK will issue the AAQ results for the full qualification at the end of Year 2 to coincide with A Level results in August and within our standard certification timeframe following the post-results appeals period.

Grade descriptors

TQUK will use the following performance descriptors to indicate the level of attainment overall across the qualification.

Grade	Descriptor
Pass	Learners show adequate recall and communication of the basic elements of much of the content being assessed. They can apply their knowledge and understanding to some basic and familiar questions, problems, or scenarios. Responses to higher order tasks involving detailed evaluation and analysis are often limited. Research, investigation, and planning of tasks are executed effectively but lack refinement, and the demonstration and application of skills and methods will produce often functional outcomes. More advanced skills and processes might be attempted but not always executed successfully. Learners will be able to review their skills, methods and actions but this may lack a detailed reflection or analysis.
Merit	Learners show good recall and communication of many elements of the content being assessed. They can sometimes develop and apply their knowledge and understanding to different questions, problems, or scenarios, including some which are more complex or less familiar. Responses to higher order tasks involving detailed evaluation and analysis are likely to be mixed, with good examples at times and others that are less detailed. Research, investigation, and planning of tasks are executed effectively and the demonstration and application of skills and methods, including those that are more advanced, are developed in range and quality. Outcomes are good quality as well as being functional. Learners will be able to review their skills, methods and actions with good application of reflection and analysis.
Distinction	Learners show thorough recall and communication of most elements of the content being assessed. They can consistently develop and apply their knowledge and understanding to different questions, problems, or scenarios, including those that are more complex or less familiar. Responses to higher-order tasks involving detailed evaluation and analysis are mostly successful. Research, investigation, and planning of tasks are executed effectively and the demonstration and application of skills and methods, including those that are more advanced, are well developed and executed. Outcomes are mostly of high quality. Learners will be able to review their skills, methods, and actions with consistent and thorough application of reflection and analysis.
Distinction*	Learners show comprehensive recall and communication of the content being assessed. They can develop and apply their knowledge and understanding to a range of complex or less familiar questions, problems, or scenarios. Research, investigation and planning of tasks are comprehensively demonstrated, and the demonstration and application of skills and methods, including those that are complex, are highly developed and executed. Outcomes are consistently highly developed and executed. Learners will be able to comprehensively review their skills, methods, and actions with comprehensive application of reflection and analysis.

Resits, Retakes, and Resubmissions

The qualification includes resit, retake, and resubmission opportunities, with availability determined by the mode of assessment and specific assessment stipulations.

Resit (EA only)

Learners are permitted resit opportunities for the Unit 1 and Unit 3 Examination Assessments (EA) as outlined in the table below:

	Year 1 May	Year 2 Jan	Year 2 May
Unit 1	First sit	Resit	Resit
Unit 3	X	First sit	Resit

Once the learner has sat the EA, their completed paper cannot be amended or improved. When the EA result is released, if a learner wishes to improve their mark, they must do so by resitting a new EA in a subsequent assessment series.

The highest mark achieved will be used to calculate the final grade.

Centres must discuss the resit process with their learners and consider any practical implications.

Retake (NEA only)

Learners may refine specific elements of their completed NEAs based on the internal feedback they receive. This provides them with a **retake** opportunity. The retake must take place **before** the final submission of the NEAs for external moderation. This process allows learners to improve their submissions, but any feedback given to them must be documented and retained by the centre. Once an NEA is submitted for external moderation, no further changes can be made to it.

Resubmission (NEA only)

A **resubmission**, in contrast to a retake, occurs **after** external moderation has taken place with **one** resubmission opportunity permitted per NEA brief (Units 2, 4, and 5).

Only learners who receive a 'Not Yet Achieved' (NYA) outcome following moderation are eligible to resubmit their NEA.

If a learner wishes to resubmit, they will be given 50% of the original supervised assessment time to complete the work for resubmission. This must be submitted by 14 June to ensure that the external moderation process is completed before final grades are awarded.

If a learner has exhausted both submission attempts on the same NEA project brief (retake and resubmission) and their evidence is graded 'Not Yet Achieved', they must complete the next live NEA project brief in the following session. In the event of a learner receiving an NYA grade, the marks achieved will count towards the overall grade.

Reviews and Appeals

TQUK is committed to ensuring any decisions it makes remain fair, reliable, and provide accurate and comparable results; however, we recognise that there may be situations where an individual wishes to appeal a decision or judgement TQUK has made.

Centres may appeal the results of the NEA moderation process. If a centre has concerns about the moderation of a cohort, it must request a review for all learners within that cohort. Written consent from all affected learners is required for the appeal to proceed.

Full details of the appeals process, including reviews of moderation, can be found in the Appeals Policy on our website.

Section 4: The NEA Moderation Process

The moderation process ensures that assessment decisions are fair, consistent, and are aligned with national standards to ensure the qualification's integrity.

In line with JCQ (Joint Council for Qualifications) regulations, our moderation process ensures that assessors have applied our marking criteria accurately across all centres and learners.

The process involves standardisation activities, the sampling of learner work, and a review of the centre-assessed marks allocated to NEA completion.

Internal standardisation and training

To maintain consistency in our assessment approach, all centres must complete standardisation training between 1 October and 28 February before marking begins. Training on administrative processes is available via Verve, with completion confirmed on conclusion of the standardisation training. Centres must sign and submit a declaration to TQUK to confirm adherence to this policy. Standardisation materials, including exemplar assessments, will be accessible from September each year.

Submission of marks and moderation

Centres must submit the learner marks awarded for the NEAs via the TQUK Portal by 30 April each year.

On 1st May, (or the next working day if this date falls on a weekend or Bank Holiday), TQUK will release to centres the list of the learners selected for moderation.

The moderation sample will be selected following the submission of all centre marks and will include learners with the lowest and highest marks and a balanced range of learners between these points. Centres are not allowed to select their own learner sample for moderation.

The moderation sample size requested adheres JCQ sampling guidelines and will be determined by the size of the learner cohort as outlined in the table below:

Number of Learners in Cohort	Sample Size Stage 1	Sample Size Stage 2	Sample Size Stage 3
Up to 5	All	All	All
6-10	5	All	All
11-15	6	10	All
16-100	6	10	15
101-200	6	15	20
Over 200	6	20	25

Centres have three working days to upload the selected learner work. Mark submission guidance is provided in the Portal User Guide to support this activity, and all learner work must be securely retained until final grades are awarded and any queries or appeals are resolved.

If all centre marks are within tolerance of the Moderator review, they will be accepted as final. If any centre marks are outside of tolerance, the moderation moves to stage 2 and the moderation sample is increased. If marking is not consistent, the sample size will be further increased as illustrated in the sampling size table.

Late submissions

A late submission will only be considered at TQUK's discretion, and extensions are only granted in exceptional cases. Centres anticipating any delays must submit a Special Consideration request. Failure to meet the deadlines may result in delays to results, ineligibility for results day, and a review of the centre's risk rating, potentially leading to compliance investigations.

External moderation process

TQUK will assign Moderators to remotely review selected samples, ensuring that the assessments align with national standards. Moderation outcomes, alongside provisional results, will be accessible to centres via the Portal.

If the centre-assigned marks and moderation outcomes are within an acceptable tolerance range, the centre's marks will be applied.

Where the marks fall outside the tolerance range, a regressed mark may be applied across the learner cohort.

If discrepancies were to persist, TQUK may request the submission of all learner work for review.

A Final Moderation Report will be provided to centres via the Portal by 14 May and will include confirmation of results, feedback on good practice, and will identify any areas of improvement.

The table below outlines the key dates relating to the moderation process.

Moderation Schedule		
Activity	**Deadline date**	**Notes**
NEA brief released	September (annually	NEA briefs are available to approved centres by Verve
Standardisation training window	1 October – 28 February	All assessors must complete standardisation using TQUK materials
Submission of learner marks	30 April	Centres must submit marks via the Portal
Release of moderation sample lists	1 May	TQUK releases a list of learners to be sampled
Upload of selected learner work	Within 3 working days of 1 May	
Resubmission deadline	14 June	

Review of NEA moderation

Following completion of a clerical check, the centre may appeal the results of the NEA moderation process. In such cases, TQUK will review the original moderation to ensure that all adjustments were applied fairly, reliably and consistently.

If a centre has concerns regarding the moderation of a specific cohort, it must request a review of moderation for all learners within that cohort. Written consent from all learners in the cohort is required for the appeal to proceed.

A review of moderation is expected to take 20 working days from when the centre formally instructs TQUK to undertake the review. TQUK will inform the centre if circumstances dictate that this timescale cannot be met.

Full details of the appeals process, including reviews of moderation, can be found in the Appeals Policy on our website.

Section 5: Appendices

Terminology

The following table defines the terminology used in this qualification specification.

Term	Definition
Examination Assessment	An externally set assessment that is internally marked and externally moderated by TQUK
Extended Response Question	An assessment question format that requires a detailed response and is often used to assess a learner's reasoning, analysis, or evaluation skills
External Moderation	The process of reviewing assessment decisions to ensure they meet accepted standards. TQUK will assign a moderator to review samples of learner work
Internal Standardisation	The process of ensuring consistency and fairness in the application of assessment decisions across assessors within a centre
Late Submission	Any submission received after the published deadline will be considered late and will only be marked at TQUK's discretion
Mark Scheme	A structured framework to determine how marks are awarded, outlining expected and acceptable answers, and the grading criteria to support grade application
Multiple Choice Question	An assessment question format where learners select the correct answer from a list of predefined options
NEA Brief	The Non-examination Assessment
Non-examination Assessment	A mode of assessment involving a project and a series of tasks that learners complete in a controlled environment in a timeframe defined by TQUK
Raw Marks	The initial score achieved before any adjustments are applied
Retake	An opportunity for a learner to reflect on their NEA and the internal feedback received and improve it **before** it has been externally moderated by TQUK.
Resubmission	An opportunity for a learner to revise and submit their work again **after** their original attempt(s) have been externally moderated by TQUK.
Short Answer Question	An assessment question format where a brief, concise response is required and is typically used to assess the recall or understanding of key facts or concepts.
Special Consideration Request	A formal application for reasonable adjustments to be put in place due to unforeseen circumstances that impact a learner's assessment performance.
Uniform Mark Scale (UMS)	A standardised scoring system that is used to convert raw marks from assessments and is used across different assessment series to support the fair comparison of results.

Verve	TQUK's management system is used by centres for learner registration, the submission of marks, and certification claims. The system is also referred to as the Portal.

Go to contents Page >

Amplification Terminology

The following table provides a selection of amplification statements used in the Alternative Academic Qualifications. This list is not exhaustive but does provide a range of commonly used statements to provide teaching staff with the intent and scope of the learning objectives.

Common amplification statements	
Characteristics and scope	**Definition**
Aspects of …	The various parts, features, or perspectives of a subject
A range of …	A collection of related items or things
The characteristics/features of …	The unique attributes or qualities of something
Common types of …	The usual classifications found within a subject
The components of …	The individual parts that combine to form a whole
The concepts of …	The ideas that are fundamental to understanding something
The elements of …	The primary components within a specific context
The fundamentals of …	The essential principles for understanding a particular subject
The types of …	The classification of different parts of a subject
The properties of …	The constituent parts or inherent characteristics of something
Function	
The contribution of …	The role something plays in achieving a result
The definition of …	The explanation or meaning of something
The function of …	The specific action or role performed by something
The principles of …	The fundamental concepts or rules underlying something
The purpose of …	The underpinning reason or intent behind something
The role of …	The specific function that something plays in a given context
Implementation	
Approaches for …	Methods or strategies for addressing a problem or achieving an objective
The application of …	The practical use or implementation of an idea or method
Considerations …	The factors to take into account
Controls when …	Measures to guide actions in certain situations
The procedures for …	The established steps for completing a task
Steps to take when …	Specific actions to be taken in a particular sequence
Strategies to …	Plan of action designed to achieve a desired result
Technical considerations …	Specific technical factors to be considered in a particular context
The use of …	The act of utilising something for a particular purpose
The ways in which …	The ways or techniques used to achieve something

Significance	
The benefits of …	The positive effects or advantages of something
The challenges associated with …	The difficulties or obstacles related to a specific topic
The criteria for …	The standards or principles used for judging or deciding something
The cultural considerations of …	Aspects related to the customs, beliefs, and social behaviour of a particular society that affects a subject
The impact / potential impact of …	The effect that something has on another
The importance of …	The significance or value of something
The meaning of …	The explanation or definition of a term or concept
A range of factors to consider when …	The elements that influence the outcome or development of something
Impact	
How X affects Y …	The direct impact one factor has on another
The consequences of …	The results or effects of or influence of an action or decision
The effects of …	The changes that result from an action
The influence of …	The capacity to have an effect on something
The implications of …	The possible future effects of a decision or action
The potential barriers to …	The factors that may hinder progress
The risks of …	The potential negative outcomes of an action
Development	
Methods of …	The ways of doing something
The origin of …	The beginning or source from which something develops
The evolution of …	The gradual change or development of something over time
The stages of …	The distinct phases or periods in a process
The structure of …	The organisation or arrangement of something
Distinctiveness	
The advantages of …	The beneficial aspects of something
The differences between …	The distinguishing characteristics between two or more things
Different ways of …	Various approaches to accomplishing something
The disadvantages of …	The unfavourable or detrimental aspects of something
The diversity of …	The variety or range of differences within a group
The limitations of …	The restricting factors or constraints of something
The positive and negative impact of …	The beneficial and detrimental effects of something
Regulatory	
Legal requirements …	The legal obligations related to something
The minimum requirements …	The lowest acceptable standards or thresholds

The responsibilities of …	The required actions and considerations
The scope of practice …	The boundaries of an individual's competence or responsibilities
Review	
Best practice for …	The most effective method or approach to achieve the desired result
The evaluation of …	The process of assessing the value or significance of something