# ICTQual AB

## Qualification Specification

# Level 2 Diploma in Information Technology Engineering 30 Credits – 3 Months

**Website**
www.ictqualab.co.uk

**Email:**
Support@ictqualab.co.uk

# ICTQual AB

# Level 2 Diploma in Information Technology Engineering 30 Credits – 3 Months

## Contents

# Qualification Specifications about

# ICTQual Level 2 Diploma in Information Technology Engineering 30 Credits – 3 Months

## About ICTQual AB

ICTQual AB UK Ltd. is a distinguished awarding body based in the United Kingdom, dedicated to fostering excellence in education, training, and skills development. Committed to global standards, ICTQual AB provides internationally recognized qualifications that empower individuals and organizations to thrive in an increasingly competitive world. Their offerings span diverse industries, including technical fields, health and safety, management, and more, ensuring relevance and adaptability to modern workforce needs.

The organization prides itself on delivering high-quality educational solutions through a network of Approved Training Centres worldwide. Their robust curriculum and innovative teaching methodologies are designed to equip learners with practical knowledge and skills for personal and professional growth. With a mission to inspire lifelong learning and drive positive change, ICTQual AB continuously evolves its programs to stay ahead of industry trends and technological advancements.

ICTQual AB's vision is to set benchmarks for educational excellence while promoting inclusivity and integrity. Their unwavering focus on quality and accessibility makes them a trusted partner in shaping future-ready professionals and advancing societal progress globally.

## Course Overview

The ICTQual Level 2 Diploma in Information Technology Engineering is a comprehensive 30-credit program designed to be completed over three months. This course provides a solid foundation in essential IT engineering concepts, including computer systems and components, networking fundamentals, and IT security and maintenance. Participants will gain practical skills in installing, configuring, and troubleshooting computer systems, setting up networks, and implementing security measures, preparing them for entry-level roles in the IT industry.

Ideal for individuals seeking to enter the rapidly evolving field of information technology, this diploma offers hands-on experience through a curriculum that balances theoretical knowledge with practical application. Graduates will be well-equipped to pursue positions such as IT support technicians, network administrators, or systems analysts. Additionally, the program serves as a stepping stone for further studies in IT or related disciplines, enhancing career prospects in the dynamic tech sector.

## Certification Framework

| | |
|---|---|
| **Qualification Title** | **ICTQual Level 2 Diploma in Information Technology Engineering 30 Credits – 3 Months** |
| **Course ID** | ITE0005 |
| **Qualification Credits** | 30 Credits |
| **Course Duration** | 3 Months |
| **Grading Type** | Pass / Fail |
| **Competency Evaluation** | Coursework / Assignments / Verifiable Experience |
| **Assessment** | The assessment and verification process for ICTQual qualifications involves two key stages:<br>**Internal Assessment and Verification:**<br>✓ Conducted by the staff at the Approved Training Centre (ATC). Ensures learners meet the required standards through continuous assessments.<br>✓ Internal quality assurance (IQA) is carried out by the centre's IQA staff to validate the assessment processes.<br>**External Quality Assurance:**<br>✓ Managed by ICTQual AB verifiers, who periodically review the centre's assessment and IQA processes.<br>✓ Verifies that assessments are conducted to the required standards and ensures consistency across centres |

## Entry Requirements

To enroll in the ICTQual Level 2 Diploma in Information Technology Engineering 30 Credits – 3 Months, candidates must meet the following entry requirements:

- ✓ Applicants must be at least 16 years old.
- ✓ A minimum of Level 1 qualification (or equivalent) in a related field such as computing, technology, or science. Alternatively, applicants should have at least GCSEs or equivalent qualifications, including Mathematics and English.
- ✓ While no prior IT engineering experience is required, applicants with a basic understanding of computer systems or technology may find the course easier to navigate.
- ✓ For non-native English speakers, proof of English language proficiency may be required.

## Qualification Structure

This qualification comprises 3 mandatory units, totaling 30 credits. Candidates must successfully complete all mandatory units to achieve the qualification.

| Mandatory Units | | |
|---|---|---|
| **Unit Ref#** | **Unit Title** | **Credits** |
| ITE0005-1 | Computer Systems and Components | 10 |
| ITE0005-2 | Networking Fundamentals | 10 |
| ITE0005-3 | IT Security and Maintenance | 10 |

## Centre Requirements

Even if a centre is already registered with ICTQual AB, it must meet specific requirements to deliver the ICTQual Level 2 Diploma in Information Technology Engineering 30 Credits – 3 Months. These standards ensure the quality and consistency of training, assessment, and learner support.

### 1. Approval to Deliver the Qualification

- ✓ Centres must obtain formal approval from ICTQual AB to deliver this specific qualification, even if they are already registered.
- ✓ The approval process includes a review of resources, staff qualifications, and policies relevant to the program.

### 2. Qualified Staff

- ✓ **Tutors:** Must have relevant qualifications in Information Technology Engineering at Level 3 or higher, alongside teaching/training experience.
- ✓ **Assessors:** Must hold a recognized assessor qualification and demonstrate expertise in Information Technology Engineering
- ✓ **Internal Quality Assurers (IQAs):** Must be appropriately qualified and experienced to monitor the quality of assessments.

### 3. Learning Facilities

Centres must have access to appropriate learning facilities, which include:

- ✓ **Classrooms:** Modern classrooms equipped with multimedia tools for delivering engaging theoretical instruction on programming, data structures, algorithms, and IT system design.
- ✓ **Practical Areas**: Advanced computer labs with high-performance systems, servers, networking equipment, and development platforms to provide hands-on experience in coding, software development, database management, and cybersecurity.
- ✓ **Technology Access:** Access to industry-standard software (e.g., Python, Java, SQL, cloud platforms) and cutting-edge tools for AI, machine learning, IoT, and big data analytics, along with reliable internet connectivity for seamless research and project work.

### 4. Health and Safety Compliance

- ✓ Centres must ensure that practical training environments comply with relevant health and safety regulations.
- ✓ Risk assessments must be conducted regularly to maintain a safe learning environment.

### 5. Resource Requirements

- ✓ Learning Materials: Approved course manuals, textbooks, and study guides aligned with the curriculum.
- ✓ Assessment Tools: Templates, guidelines, and resources for conducting and recording assessments.
- ✓ E-Learning Systems: If offering online or hybrid learning, centres must provide a robust Learning Management System (LMS) to facilitate remote delivery.

### 6. Assessment and Quality Assurance

- ✓ Centres must adhere to ICTQual's assessment standards, ensuring that all assessments are fair, valid, and reliable.
- ✓ Internal quality assurance (IQA) processes must be in place to monitor assessments and provide feedback to assessors.
- ✓ External verification visits from ICTQual will ensure compliance with awarding body standards.

### 7. Learner Support

- ✓ Centres must provide learners with access to guidance and support throughout the program, including:
- ✓ Academic support for coursework.
- ✓ Career guidance for future progression.
- ✓ Additional support for learners with specific needs (e.g., disabilities or language barriers).

### 8. Policies and Procedures

Centres must maintain and implement the following policies, as required by ICTQual:

- ✓ Equal Opportunities Policy.
- ✓ Health and Safety Policy.
- ✓ Safeguarding Policies and Procedures.
- ✓ Complaints and Appeals Procedure.
- ✓ Data Protection and Confidentiality Policy.

### 9. Regular Reporting to ICTQual

- ✓ Centres must provide regular updates to ICTQual AB on learner enrollment, progress, and completion rates.
- ✓ Centres are required to maintain records of assessments and learner achievements for external auditing purposes.

## Support for Candidates

Centres should ensure that materials developed to support candidates:

- ✓ Facilitate tracking of achievements as candidate's progress through the learning outcomes and assessment criteria.
- ✓ Include information on how and where ICTQual's policies and procedures can be accessed.
- ✓ Provide mechanisms for Internal and External Quality Assurance staff to verify and authenticate evidence effectively.

This approach ensures transparency, supports candidates' learning journeys, and upholds quality assurance standards.

## Assessment

This qualification is competence-based, requiring candidates to demonstrate proficiency as defined in the qualification units. The assessment evaluates the candidate's skills, knowledge, and understanding against the set standards. Key details include:

1. **Assessment Process:**

   - ✓ Must be conducted by an experienced and qualified assessor.
   - ✓ Candidates compile a portfolio of evidence that satisfies all learning outcomes and assessment criteria for each unit.

2. **Types of Evidence:**

   - ✓ Observation reports by the assessor.
   - ✓ Assignments, projects, or reports.
   - ✓ Professional discussions.
   - ✓ Witness testimonies.
   - ✓ Candidate-produced work.
   - ✓ Worksheets.
   - ✓ Records of oral and written questioning.
   - ✓ Recognition of Prior Learning (RPL).

3. **Learning Outcomes and Assessment Criteria:**

   - ✓ **Learning Outcomes:** Define what candidates should know, understand, or accomplish upon completing the unit.
   - ✓ **Assessment Criteria:** Detail the standards candidates must meet to demonstrate that the learning outcomes have been achieved.

This framework ensures rigorous and consistent evaluation of candidates' competence in line with the qualification's objectives.

## Unit Descriptors

**ITE0005 -1 Computer Systems and Components**

The aim of this unit is to provide learners with a foundational understanding of computer systems, focusing on the key components such as hardware, software, and operating systems. Learners will develop the skills to install, configure, and troubleshoot basic computer systems and peripherals. The unit will also cover diagnostic techniques for identifying and resolving hardware and software issues, allowing learners to effectively maintain and optimize systems.

| Learning Outcome: | Assessment Criteria: |
|---|---|
| **1. Understand the key components of computer systems, including hardware, software, and operating systems.** | 1.1. Demonstrate an understanding of the fundamental components of a computer system, including hardware, software, and operating systems.<br>1.2. Identify the primary hardware components of a computer, such as the central processing unit (CPU), memory (RAM), storage devices, and peripheral devices, and describe their roles in system operation.<br>1.3. Explain the purpose and types of software, differentiating between system software (e.g., operating systems) and application software (e.g., productivity tools, web browsers).<br>1.4. Describe the key functions of an operating system, including resource management, user interface provision, and control of hardware and software interactions.<br>1.5. Analyze the relationship between hardware and software, and how the operating system acts as an intermediary between the two.<br>1.6. Assess the role of drivers and firmware in ensuring the compatibility between hardware components and the operating system.<br>1.7. Understand the boot process, including the role of BIOS/UEFI and the loading of the operating system into memory.<br>1.8. Demonstrate the ability to troubleshoot basic hardware and software issues by understanding the interplay between these components.<br>1.9. Evaluate how hardware and software evolve over time to meet the growing demands of users and applications. |
| **2. Demonstrate the ability to install, configure,** | 2.1. Successfully install operating systems (e.g., |

| | |
|---|---|
| **and troubleshoot basic computer systems and peripherals.** | Windows, Linux) on a computer system, ensuring hardware components such as CPU, RAM, and storage devices are properly recognized and configured.<br>2.2. Set up basic computer peripherals (e.g., monitors, keyboards, printers) and ensure proper connection and operational status, including driver installation and optimal configuration.<br>2.3. Configure system settings such as network connections (Wi-Fi, Ethernet), user accounts, and security settings like antivirus software, firewalls, and system updates.<br>2.4. Install essential software applications (e.g., productivity software, browsers) and ensure proper installation, configuration, and updates while managing software dependencies.<br>2.5. Troubleshoot common hardware issues such as malfunctioning peripherals, damaged components (e.g., hard drives, power supply units), or connection interface problems (e.g., USB, HDMI).<br>2.6. Resolve software-related problems, such as system crashes, slow performance, or operating system errors, using built-in troubleshooting tools (e.g., task manager, system restore).<br>2.7. Diagnose and resolve peripheral issues such as printers, mice, or monitors, including checking connections, reinstalling drivers, and testing with different systems if necessary.<br>2.8. Optimize system performance through settings adjustments (e.g., power management, display settings) and performing system maintenance tasks like disk cleanup and updating drivers.<br>2.9. Provide clear instructions for installation, configuration, and troubleshooting, as well as offer support to end-users for resolving basic system and peripheral issues. |
| **3. Apply diagnostic techniques to identify and resolve hardware and software issues.** | 3.1. Use diagnostic tools such as system logs, built-in hardware diagnostics, and software error reports to identify specific hardware or software issues.<br>3.2. Perform basic troubleshooting steps such as rebooting the system, checking for loose |

| | |
|---|---|
| | connections, or confirming power supply status to address potential hardware failures.<br>3.3. Apply system utilities (e.g., Task Manager, Device Manager) to check for software performance issues, system processes, or hardware malfunctions, and identify faulty drivers or system errors.<br>3.4. Use hardware testing tools (e.g., memtest86 for RAM, CrystalDiskInfo for hard drives) to evaluate the health and functionality of physical components like memory and storage devices.<br>3.5. Employ software-specific diagnostic techniques, such as reinstalling or updating software, to resolve issues caused by corrupt or outdated applications.<br>3.6. Troubleshoot network connectivity issues using tools like ping, tracert, or ipconfig to verify IP configurations and identify potential issues with network hardware or software.<br>3.7. Perform operating system repairs, such as running System File Checker (sfc /scannow) or restoring from system backups, to resolve system corruption or missing files.<br>3.8. For peripheral issues, systematically isolate the problem by testing devices with different systems, checking drivers, and ensuring compatibility with the operating system.<br>3.9. Analyze error messages and blue screen codes for deeper insights into underlying hardware or software issues and apply appropriate solutions based on diagnostic results. |
| **4. Develop an understanding of system maintenance and optimization processes.** | 4.1. Regularly updating operating systems, drivers, and software ensures compatibility with the latest security protocols and bug fixes. This helps prevent security vulnerabilities and ensures smooth system performance. Automating updates can reduce the risk of missing critical patches.<br>4.2. Periodically clearing unnecessary files, such as temporary files, caches, and system logs, can free up space and optimize storage performance. Defragmentation, particularly for HDDs, helps organize fragmented data for faster access.<br>4.3. Using system monitoring tools to track CPU usage, memory consumption, and disk activity allows early detection of performance |

| | |
|---|---|
| | bottlenecks. Regular checks can help identify unnecessary processes or resource hogs that slow down the system.<br>4.4. Physical maintenance, such as cleaning dust from vents and components, ensures the hardware runs efficiently and prevents overheating. Replacing or upgrading hardware components, like adding more RAM or swapping out hard drives for SSDs, can significantly enhance system performance.<br>4.5. Regularly backing up data ensures that in the event of a system failure, important files and configurations are recoverable. A comprehensive backup strategy includes both system files and user data, with off-site or cloud-based backups for extra security.<br>4.6. Ongoing monitoring for security threats, using antivirus software, firewalls, and encryption techniques, is vital for maintaining system integrity. Regular scans for malware and ensuring that security software definitions are up-to-date are essential steps for maintaining a secure environment.<br>4.7. Tweaking system settings, like startup programs, visual effects, and power settings, can improve system responsiveness and energy efficiency. Tools such as Windows' built-in Performance Options or third-party utilities can assist in making these adjustments.<br>4.8. Streamlining background processes and services, minimizing the number of running applications, and configuring system settings for optimal performance can improve speed. Optimization may also involve adjusting the system's power settings for performance versus energy saving depending on the user's needs.<br>4.9. Managing user permissions, deleting unused accounts, and ensuring proper access control contribute to both security and performance. Limiting access to essential applications and features reduces the risk of accidental or intentional system alterations. |

**ITE0005 -2 Networking Fundamentals**

The aim of this unit is to provide learners with a comprehensive understanding of networking concepts, including the different types of networks such as Local Area Networks (LAN) and Wide Area Networks (WAN). Learners will explore the role of network protocols in facilitating communication between devices and gain hands-on experience in setting up and configuring basic networking devices, such as routers and switches.

| Learning Outcome: | Assessment Criteria: |
|---|---|
| **1. Identify and describe different types of networks (LAN, WAN) and their components.** | 1.1. A LAN (Local Area Network) is a network confined to a small geographical area like a home, office, or building. It typically uses Ethernet cables or Wi-Fi for communication. LAN components include switches for connecting multiple devices, routers for linking to external networks, access points for wireless connections, and network interface cards (NICs) for device connectivity.<br>1.2. A WAN (Wide Area Network) spans large geographical areas, such as cities or countries. It connects multiple LANs and can cover vast distances, including international connections. Components of a WAN include routers and gateways for routing data, transmission media like fiber optics or satellite links for long-distance communication, repeaters and amplifiers for signal boosting, and modems for modulating data for transmission over various media.<br>1.3. The primary difference is the scale and geographical reach, with LANs offering faster and more secure communication within a small area, while WANs handle communication over long distances but may experience higher latency. Both types of networks rely on foundational components such as routers, switches, and transmission media but differ in their application and infrastructure. |
| **2. Understand network protocols and their role in facilitating communication between devices.** | 2.1. Network protocols are essential rules and standards that allow different devices and systems to communicate with each other over a network. They ensure data is transferred efficiently, securely, and in a format that can be understood by both the sender and the receiver.<br>2.2. Transmission Control Protocol (TCP) ensures reliable data transmission by establishing a connection between devices, checking for errors, and confirming that packets have been |

| | |
|---|---|
| | received correctly.<br>2.3. Internet Protocol (IP) is responsible for addressing and routing data packets so that they reach the correct destination device within a network.<br>2.4. Hypertext Transfer Protocol (HTTP) is used for communication between web browsers and servers, allowing for the retrieval of web pages.<br>2.5. File Transfer Protocol (FTP) facilitates the transfer of files between systems over a network, allowing users to upload or download files.<br>2.6. Simple Mail Transfer Protocol (SMTP) is used for sending emails between servers, while Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) allow for receiving and managing emails.<br>2.7. Each protocol has a specific function that ensures seamless communication across different devices and platforms. They define how data is formatted, transmitted, and received, and they play a critical role in maintaining the integrity and security of network interactions. |
| **3. Set up and configure basic networking devices (e.g., routers, switches) and troubleshoot common network issues.** | 3.1. Demonstrate the ability to physically connect basic networking devices, such as routers and switches, ensuring proper cabling and port connections.<br>3.2. Access and configure the web interface or command-line interface (CLI) of routers and switches to set up network parameters, including IP addressing, DHCP, and wireless settings (for routers).<br>3.3. Configure network devices for optimal performance, ensuring appropriate settings for IP addressing (static or dynamic), subnetting, and default gateway configurations.<br>3.4. Implement basic security measures, such as setting up strong administrator passwords, configuring network encryption for Wi-Fi and enabling firewall features on routers.<br>3.5. Troubleshoot and resolve connectivity issues by checking the status indicators on devices (LEDs), verifying cable connections, and rebooting the devices when necessary.<br>3.6. Identify and address IP address conflicts within a network by assigning static IP addresses or adjusting DHCP settings to avoid overlap. |

| | |
|---|---|
| | 3.7. Test connectivity between network devices using tools such as ping, tracert, or network diagnostic utilities to identify routing or connection issues.<br>3.8. Perform firmware updates and maintain up-to-date device configurations to ensure optimal functionality and security of networking devices.<br>3.9. Troubleshoot network performance issues by identifying bottlenecks, checking for faulty cables, or reviewing router and switch logs to detect potential errors or misconfigurations. |
| **4. Apply fundamental network security practices to protect data and ensure network reliability.** | 4.1. Implement basic firewalls and intrusion detection/prevention systems (IDS/IPS) to filter malicious traffic and monitor unauthorized network access attempts.<br>4.2. Configure network access control lists (ACLs) to restrict and manage access to specific devices or segments of the network, ensuring that only authorized devices are allowed to communicate.<br>4.3. Use encryption techniques, such as SSL/TLS for securing data in transit and WPA2 or WPA3 for wireless networks, to protect data confidentiality and integrity.<br>4.4. Regularly update and patch network devices and software to protect against known vulnerabilities and ensure the latest security features are in place.<br>4.5. Set up strong authentication methods, including multi-factor authentication (MFA) and the use of complex passwords, to secure network access.<br>4.6. Perform regular security audits and vulnerability assessments to identify and mitigate potential weaknesses in the network infrastructure.<br>4.7. Enable logging and monitoring on network devices to track activity and detect unusual or suspicious behaviors that may indicate a security breach.<br>4.8. Segment the network using VLANs to reduce the attack surface and prevent lateral movement of attackers within the network.<br>4.9. Implement proper backup strategies for network configurations and data, ensuring that in case of a security breach or system failure, recovery is possible. |

**ITE0005 -3 IT Security and Maintenance**

The aim of this unit is to equip learners with the foundational knowledge and skills necessary to protect computer systems and networks from common IT security threats and vulnerabilities. Learners will gain an understanding of key security principles and be trained to implement essential security measures such as encryption, firewalls, and antivirus software. The unit will also cover best practices for routine system maintenance to ensure optimal performance, including performing updates and backups.

| Learning Outcome: | Assessment Criteria: |
|---|---|
| **1. Understand the key principles of IT security, including common threats and vulnerabilities.** | 1.1. Confidentiality ensures that only authorized individuals can access sensitive information, employing measures like encryption, secure passwords, and access controls.<br>1.2. Integrity maintains data accuracy and prevents unauthorized changes, with techniques like data hashing and digital signatures.<br>1.3. Availability ensures that systems and data are accessible when needed, supported by redundancy, backup systems, and fault tolerance.<br>1.4. Authentication verifies the identity of users or devices before granting access, utilizing methods such as multi-factor authentication (MFA) and biometrics.<br>1.5. Authorization ensures users can only access resources they are permitted to, often enforced through role-based access control (RBAC).<br>1.6. Non-repudiation ensures actions cannot be denied after they are performed, achieved by logging activities and using digital signatures.<br>1.7. Common security threats include malware, phishing, DoS attacks, and data breaches, while vulnerabilities refer to weaknesses in systems or software that attackers can exploit.<br>1.8. IT security involves constant monitoring for potential threats and applying updates and patches to close security gaps, alongside educating users on best practices for safe data handling and interaction. |
| **2. Implement basic security measures, such as encryption, firewalls, and antivirus software, to protect computer systems and networks.** | 2.1. Understand the importance of encryption techniques to secure data transmission and storage, using algorithms like AES for encryption and RSA for secure key exchange.<br>2.2. Implement and configure firewalls to monitor and control incoming and outgoing network traffic based on predefined security rules, |

| | |
|---|---|
| | blocking unauthorized access.<br>2.3. Apply antivirus software to scan, detect, and remove malware, ensuring ongoing protection of systems and networks from viruses, trojans, worms, and ransomware.<br>2.4. Configure and maintain Virtual Private Networks (VPNs) to establish secure, encrypted communication channels for remote users accessing internal network resources.<br>2.5. Enforce access control mechanisms, including multi-factor authentication (MFA) and role-based access control (RBAC), to ensure only authorized users can access sensitive data.<br>2.6. Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious activities and mitigate potential threats in real time.<br>2.7. Regularly update software and firmware, including security patches and updates, to minimize vulnerabilities and ensure systems are protected against the latest threats.<br>2.8. Ensure the use of strong password policies and techniques, including password complexity requirements, expiration, and encryption, to protect access to systems and data.<br>2.9. Implement security auditing and logging practices to track and analyze network activity for signs of potential security breaches, aiding in proactive threat mitigation. |
| **3. Perform routine maintenance tasks to ensure optimal system performance, including updates and backups.** | 3.1. Regularly apply software and security updates, including OS patches, application updates, and driver installations, to maintain system integrity and security.<br>3.2. Perform routine disk cleanup by removing temporary files, old logs, and unused data to free up storage and maintain performance.<br>3.3. Implement automated, regular backups of system data, settings, and applications to ensure disaster recovery readiness.<br>3.4. Continuously monitor system performance, focusing on CPU, memory, and network usage to detect potential bottlenecks or issues.<br>3.5. Run defragmentation tools for traditional hard drives (HDDs) to optimize file access and reduce system latency.<br>3.6. Conduct regular malware scans with antivirus |

| | |
|---|---|
| | software to identify and mitigate security threats that may compromise performance.<br>3.7. Clear cache files and browser histories to prevent accumulation of redundant data that may slow down the system.<br>3.8. Review user accounts and permissions regularly to ensure access control is maintained, reducing the risk of unauthorized access.<br>3.9. Test the integrity of backups periodically and perform restore simulations to ensure data recovery processes work as expected. |
| **4. Understand and apply data protection and recovery strategies in case of system failure or data loss.** | 4.1. Identify critical data and categorize it to prioritize protection during backup and recovery.<br>4.2. Implement regular and automated backups to external or cloud storage to protect data from local failures.<br>4.3. Use appropriate backup schedules (e.g., daily, weekly) and maintain version control for multiple data recovery states.<br>4.4. Encrypt backup data to ensure the protection of sensitive information during storage and transfer.<br>4.5. Define recovery point objectives (RPO) and recovery time objectives (RTO) to set clear data loss and downtime goals.<br>4.6. Develop and regularly update a disaster recovery plan with procedures for restoring systems and data.<br>4.7. Conduct regular recovery drills to test and ensure the functionality and efficiency of backup and restoration processes.<br>4.8. Leverage cloud-based storage and recovery solutions for scalable, off-site backups and improved system resilience.<br>4.9. Ensure compliance with relevant data protection laws (e.g., GDPR, HIPAA) to avoid legal risks while implementing backup strategies. |

## ICTQual AB

Yew Tree Avenue, Dagenham,

London East,United Kingdom RM10 7FN

+44 744 139 8083

Support@ictqualab.co.uk | www.ictqualab.co.uk

**Visit Official Web page**