GCE A LEVEL MARKING SCHEME

SUMMER 2025

A LEVEL
DIGITAL TECHNOLOGY - UNIT 3
1540U30-1

About this marking scheme

The purpose of this marking scheme is to provide teachers, learners, and other interested parties, with an understanding of the assessment criteria used to assess this specific assessment.

This marking scheme reflects the criteria by which this assessment was marked in a live series and was finalised following detailed discussion at an examiners' conference. A team of qualified examiners were trained specifically in the application of this marking scheme. The aim of the conference was to ensure that the marking scheme was interpreted and applied in the same way by all examiners. It may not be possible, or appropriate, to capture every variation that a candidate may present in their responses within this marking scheme. However, during the training conference, examiners were guided in using their professional judgement to credit alternative valid responses as instructed by the document, and through reviewing exemplar responses.

Without the benefit of participation in the examiners' conference, teachers, learners and other users, may have different views on certain matters of detail or interpretation. Therefore, it is strongly recommended that this marking scheme is used alongside other guidance, such as published exemplar materials or Guidance for Teaching. This marking scheme is final and will not be changed, unless in the event that a clear error is identified, as it reflects the criteria used to assess candidate responses during the live series.

WJEC GCE AS DIGITAL TECHNOLOGY – UNIT 3

SUMMER 2025 MARK SCHEME

Question		Answer	AO1	AO2	Total
1	*(a)*	*Describe different purposes of collecting data.*			

		Indicative content
		• Conducting research and building knowledge
		  ○ To explore questions, test hypotheses, and expand understanding in academic, scientific, or applied fields.
		• Supporting informed decision-making
		  ○ To guide strategic and operational choices based on evidence and trends.
		• Solving problems and identifying root causes
		  ○ To diagnose issues and determine effective solutions.
		• Allocating resources effectively
		  ○ To distribute budgets, personnel, and assets based on need and impact.
		• Evaluating performance
		  ○ To assess efficiency, productivity, and outcomes within organisations or systems.
		• Benchmarking against standards or competitors
		  ○ To compare performance and identify areas of strength or improvement.
		• Ensuring quality and standards compliance
		  ○ To maintain product or service quality through testing, monitoring, and feedback.
		• Managing risks
		  ○ To detect and mitigate potential threats in areas like finance, health, and safety.
		• Meeting compliance and reporting obligations
		  ○ To fulfil regulatory requirements through accurate data reporting.
		• Monitoring trends and activities
		  ○ To observe developments in environments, populations, or systems in real time.
		• Forecasting future events or demands
		  ○ To predict upcoming trends, needs, or behaviours based on historical and real-time data.
		• Developing policies and regulations
		  ○ To inform evidence-based governance and public sector planning.
		• Planning economic strategies
		  ○ To guide decisions on fiscal policy, trade, and national or regional development.
		• Gaining customer and market insights
		  ○ To understand consumer behaviour and improve products, services, and marketing.
		• Training algorithms and AI models
		  ○ To enable machine learning systems to recognise patterns, make predictions, or
			6		6

Question		Answer	AO1	AO2	Total

		automate decisions.
		• Supporting personalisation
		  ○ To tailor user experiences, recommendations, and services based on individual data.
		• Facilitating communication and engagement
		  ○ To segment audiences and improve outreach in marketing, public services, or education.
		• Tracking progress towards goals or KPIs
		  ○ To monitor success in relation to predefined targets in projects, policies, or programmes.			

Band	AO1
3	**5 – 6 marks** A very good description, which shows: • thorough knowledge and understanding of the different purposes of collecting data • a confident grasp of the different purposes of collecting data.
2	**3 - 4 marks** A good description, which shows: • generally secure knowledge and understanding of the different purposes of collecting data • a generally secure grasp of the different purposes of collecting data.
1	**1 - 2 marks** A basic description, which shows: • some knowledge and understanding of the different purposes of collecting data • some grasp of the different purposes of collecting data.
	0 marks • response not creditworthy or not attempted.

Question		Answer	AO1	AO2	Total
	(b)	*Suggest two appropriate ways of collecting data.*			
		Award up to three marks for each method, up to a maximum of six marks • Autonomous devices o Autonomous devices collect data automatically without human intervention o Examples include sensors, automated data loggers, and autonomous drones used in various industries. • Passive data collection o Passive data collection involves gathering data without direct interaction with participants o Examples include monitoring web traffic or analysing existing records • Active data collection o Active data collection requires direct engagement with participants o Examples include conducting surveys or interviews. • Manual data collection o Manual data collection involves individuals or researchers recording data by hand or through manual processes o Examples include filling out paper surveys, taking field notes, or transcribing audio recordings. • Usage data o Usage data refers to information collected about how individuals interact with a product, service, or technology o This data can include website analytics, app usage statistics, or how customers engage with a product, providing insights into user behaviour. *Accept any other reasonable expansion for each method*	6		6

Question		Answer	AO1	AO2	Total
2	*Parkwood Vale Bank is an international banking institution that takes cyber security very seriously*				
	(a)	*Consider a range of security measures that Parkwood Vale Bank may use to protect its customers' data.*			

		Indicative content
		
		• Encryption
		  ○ Encryption is essential for protecting sensitive financial data, such as customer account information, transactions, and communication between branches and external partners
		  ○ All data transmitted over the network, including online banking transactions and customer information, is encrypted to prevent unauthorised access.
		• Firewalls
		  ○ Firewalls are used to safeguard the financial institution's network infrastructure from external threats
		  ○ They block unauthorised access, filter network traffic, and prevent malicious intrusions, helping to protect customer data and the integrity of financial operations.
		• Antivirus software
		  ○ Antivirus software is crucial for detecting and removing malware, which can be used to compromise systems and steal sensitive financial data
		  ○ It scans all devices within the organisation, including employee workstations and servers, to ensure they are free from viruses and other malicious software.
		• Access levels
		  ○ In a financial institution, there are different levels of access to sensitive information
		  ○ For example, staff may have access to customer account balances, while loan officers might have access to loan application data
		  ○ Implementing hierarchical access levels ensures that employees only have access to the information necessary for their roles, preventing unauthorised access and reducing the risk of data breaches.
		
		Accept VPN, MFA and staff training
		
		NOT backups
				6	6

Question	Answer	AO1	AO2	Total

Band	AO2
3	**5 – 6 marks** A very good consideration, which shows: • thorough knowledge and understanding of a range of security measures • a confident grasp of the different security measures available to Parkwood Vale Bank.
2	**3 - 4 marks** A good consideration, which shows: • generally secure knowledge and understanding of a range of security measures • a generally secure grasp of the different security measures available to Parkwood Vale Bank.
1	**1 - 2 marks** A basic consideration, which shows: • some knowledge and understanding of a range of security measures • some grasp of the different security measures available to Parkwood Vale Bank.
	0 marks • response not creditworthy or not attempted.

	(b)	*Explain the legal and professional responsibilities of Parkwood Vale Bank in identifying and mitigating cyber security threats*			

		Indicative content
		
		Legal Responsibilities
		
		• Compliance with data protection laws
		  ○ Organisations must follow data protection laws (like GDPR or Data Protection Act) to protect personal and sensitive data.
		• Data security and privacy
		  ○ Legally required to keep personal data secure, accurate, and used fairly. It must only be kept as long as necessary.
		• Incident reporting
		  ○ Must report serious data breaches to a relevant authority (e.g. the ICO) within a set time (e.g. 72 hours for GDPR).
		• Business continuity
		  ○ Legally expected to have plans to recover quickly from cyberattacks and keep essential services running.
		
		Professional Responsibilities
		
		• Protecting customer data
		  ○ Professionals must handle and store data securely and responsibly to maintain customer trust.
		• Staff training
		  ○ IT staff should be trained in recognising risks like
				6	6

Question		Answer	AO1	AO2	Total

		phishing, social engineering, and following secure processes.
		• Using secure systems
		  ○ Expected to use reliable technologies (like antivirus software, firewalls, encryption) to prevent unauthorised access.
		• Monitoring and regular reviews
		  ○ Systems and defences should be checked regularly, and issues should be fixed quickly.
		• Incident response plan
		  ○ Maintaining a clear, tested plan for how to detect, respond to, and recover from cyber attacks or breaches.
		• Ethical handling of data
		  ○ Professionals should be honest, transparent, and fair in how they manage digital information.			

Band	AO2
3	**5 - 6 marks** A very good explanation, which shows: • thorough knowledge and understanding of the legal **and** professional responsibilities • a confident grasp of their role in mitigating cyber security threats.
2	**3 - 4 marks** A good explanation, which shows: • generally secure knowledge and understanding of the legal **and/or** professional responsibilities • a generally secure grasp of their role in mitigating cyber security threats.
1	**1 - 2 marks** A basic explanation, which shows: • some knowledge and understanding of the legal **or** professional responsibilities • some grasp of their role in mitigating cyber security threats.
	0 marks • response not creditworthy or not attempted.

Question		Answer	AO1	AO2	Total
3	*A Hospital Management Information System (HMIS) is a specialised MIS that supports decision-making at various levels in the health sector, both medical and administrative.*				
	(a)	*Discuss the role of the HMIS in supporting decision making.*			

		Indicative content
		• Clinical decision support
		  ○ Stores and provides patient data to assist healthcare professionals in making accurate diagnoses and treatment choices.
		• Resource allocation
		  ○ Tracks usage of human and material resources to help optimise staffing, equipment, and facility management.
		• Financial management
		  ○ Facilitates budgeting, expenditure tracking, and financial planning for cost-effective healthcare delivery.
		• Quality improvement
		  ○ Monitors clinical outcomes, regulatory compliance, and patient satisfaction to support continuous service enhancement.
		• Inventory management
		  ○ Manages medical supplies and equipment stock levels to minimise waste and prevent shortages.
		• Strategic planning
		  ○ Supports long-term policy and operational planning using trends in population health and service utilisation.
		• Reporting and analytics
		  ○ Generates detailed reports and dashboards for data-driven decisions across clinical, operational, and administrative areas.
				4	4

Band	AO2
3	**4 marks** A very good discussion, which shows: • thorough knowledge and understanding of HMIS • a confident grasp of their role in supporting decision making.
2	**2 - 3 marks** A good discussion, which shows: • generally secure knowledge and understanding of HMIS • a generally secure grasp of their role in supporting decision making.
1	**1 mark** A basic discussion, which shows: • some knowledge and understanding of HMIS • some grasp of their role in supporting decision making.
	0 marks • response not creditworthy or not attempted.

Question		Answer	AO1	AO2	Total
	(b)	*All devices that belong to the sector are connected to their network.*			
	(i)	*Describe the characteristics of the following contemporary communication infrastructures:* • *twisted pair wire (UTP and STP)* • *fibre optic cable.*			
		Award up to three marks for twisted pair wire and up to three marks for fibre optic cable **Twisted pair wire** • UTP has no shielding. STP includes shielding to reduce interference • Common in Ethernet, phone lines, or local area networks • Susceptible to interference, limited range, lower bandwidth • Cheap, easy to install, flexible, used for short distances indoors • Less durable, affected by EMI, slower than fibre optic. **Fibre optic cable** • Uses light signals, made of glass or plastic fibres • High speed, high bandwidth, can transmit over long distances • Immune to EMI, very secure, durable, low signal loss • Used in hospitals, ISPs, telecoms, data centres • Expensive to install, harder to repair. Accept real-world application examples in healthcare or general networking.	3 3		6
	(ii)	*Describe the role and facilities provided by network activity management software.*			
		Award one mark for the role • Manage and monitor the performance of a network • Support risk management, performance, or security • Ensure smooth and reliable network operation **Award one mark for each of the following, up to a maximum of three marks** • Monitoring and detection - Continuous traffic monitoring, intrusion detection, tracking abnormal activity • Traffic/resource management - Preventing congestion, traffic shaping, prioritising data flow • Performance analysis and reporting - Analysing performance, generating reports, identifying issues • Capacity planning and alerts - Planning for growth, issuing alerts, managing from a distance • Security and auditing - Logging access, tracking user behaviour, supporting compliance.	1 3		4

Question		Answer	AO1	AO2	Total
4	*(a)*	*Describe Artificial Intelligence.*			
		Award one mark for each of the following up to a maximum of four marks • Definition - Artificial Intelligence refers to the simulation of human intelligence processes by machines, especially computer systems. • Core capabilities - Includes functions such as learning (machine learning), reasoning, problem-solving, perception, and language understanding. Types of AI • Narrow AI - Designed for specific tasks (e.g. voice assistants, recommendation systems). • General AI - Hypothetical AI with human-level intelligence across a broad range of tasks. • Superintelligent AI - A theoretical future AI that surpasses human intelligence. • Machine learning - A major subset where algorithms learn from data to improve performance without being explicitly programmed. • Deep learning - A specialised form of machine learning that uses neural networks to model complex patterns, often used in image and speech recognition. • Natural language processing (NLP) - Enables machines to understand, interpret, and generate human language. • Computer vision - Allows machines to interpret visual information from the world, such as recognising faces or objects. • Autonomy - AI systems can operate independently to make decisions or perform tasks (e.g. self-driving cars). • Applications - Used in fields such as healthcare, finance, manufacturing, education, entertainment, and defence. • Data dependence - AI systems require large amounts of data to learn and make accurate decisions. • Ethical considerations - Raises concerns about bias, privacy, job displacement, accountability, and control. • Human-AI interaction - Involves how humans and AI systems work together, including user interfaces and decision support. • Evolving nature - AI is constantly advancing, with research pushing boundaries in creativity, emotional intelligence, and reasoning.	4		4

Question		Answer	AO1	AO2	Total
	(b)	*Outline the main principles of the Turing test*			
		Indicative content • Purpose - it tests a machine's ability to show human-like intelligence • Participants - includes a human judge, a human participant, and a machine • Interaction method - communication is via text only to avoid visual/auditory clues • Passing condition - if the judge can't tell which is which, the machine passes • Focus on simulation - the test measures how well AI can simulate human responses, not true intelligence • Limitations - may not measure full intelligence -only language and conversation	6		6

Band	AO1
3	**5 – 6 marks** A very good description, which shows: • thorough knowledge and understanding of the Turing test • a confident grasp of the main principles of the Turing test
2	**3 - 4 marks** A good description, which shows: • generally secure knowledge and understanding of the Turing test • a generally secure grasp of the main principles of the Turing test.
1	**1 - 2 marks** A basic description, which shows: • some knowledge and understanding of the Turing test • some grasp of the main principles of the Turing test.
	0 marks • response not creditworthy or not attempted.

Question	Answer	AO1	AO2	Total
5	*Parkwood Vale Engineering uses quality control in manufacturing. The use of expert systems can be highly beneficial for improving the quality assurance processes.* *Explain shell, heuristics and fuzzy logic in relation to Parkwood Vale Engineering's expert system.*			
	Award one mark for each basic response, up to a maximum of three marks **Award two marks for each good response, up to a maximum of six marks** Shell • Basic: Identifies the shell as the user interface or framework that allows interaction with the expert system • Good: Explains that the shell includes user interface, inference engine, and links to the knowledge base. May mention customisation for engineering use (e.g. entering data, viewing results) Heuristics • Basic: States heuristics are guidelines or rules used by the system to make decisions • Good: Explains heuristics as rules of thumb based on human experience or pattern recognition. Describes how they help the system solve problems when exact rules aren't available. Fuzzy Logic • Basic: Mentions fuzzy logic deals with uncertainty or imprecise information • Good: Explains fuzzy logic evaluates data on a scale (e.g. "partially faulty" or "mostly acceptable"). Recognises it supports graded decisions, not just yes/no outcomes		3 3	6

Question		Answer	AO1	AO2	Total
6	*The proliferation of mobile phone technology refers to the widespread adoption and expansion of mobile phones and their associated technologies.*				
	(a)	*Describe the following impacts of the proliferation of mobile technologies:*			
	(i)	*social impact.*			

		Award one mark for each impact, up to a maximum of three marks
		• Increased connectivity and communication
		  ○ People can stay in touch across distances instantly, enhancing personal and professional relationships.
		• Changes in social behaviour and interaction
		  ○ Face-to-face interaction has often decreased, with many relying more on digital communication.
		• Greater access to information and services
		  ○ Mobile devices provide instant access to news, education, healthcare, and public services, narrowing information gaps.
		• Digital inclusion and exclusion
		  ○ While many benefit from mobile technology, those without access face increased social and economic marginalisation.
		• Shifts in work and employment patterns
		  ○ Mobile tech supports remote working and gig economy jobs, changing how and where people work.
		• Impacts on mental health and well-being
		  ○ Overuse or dependence on mobile devices can contribute to anxiety, sleep disruption, and reduced attention spans.
		• Enhanced civic engagement and activism
		  ○ Social movements and campaigns can mobilise quickly through mobile platforms, increasing public participation.
		• Privacy and surveillance concerns
		  ○ The widespread use of mobile tech raises issues around data collection, location tracking, and personal privacy.
		• Transformation of consumer behaviour
		  ○ Mobile access has changed how people shop, bank, and consume media, shifting power towards more personalised experiences.
		• Cultural change and globalisation
		  ○ Mobile technologies spread global culture rapidly, sometimes challenging local traditions and identities.
		
		Accept any other valid response.
			3		3

Question		Answer	AO1	AO2	Total
	(ii)	*environmental impact.*			
		Award one mark for each impact, up to a maximum of three marks • Electronic waste (e-waste) - The rapid turnover of mobile devices leads to a growing volume of discarded phones, batteries, and accessories, much of which is not properly recycled. • Resource extraction - Mobile phones require rare earth elements and precious metals, leading to environmentally damaging mining operations and habitat destruction. • Energy consumption - The production, use, and charging of mobile devices, as well as the operation of data centres and mobile networks, contribute to increased energy demand and carbon emissions. • Pollution from manufacturing - The production process involves toxic chemicals and produces industrial waste that can contaminate air, water, and soil if not managed properly. • Greenhouse gas emissions - From manufacturing to transport and usage, the mobile technology lifecycle emits significant amounts of CO_2 and other greenhouse gases. • Short device lifespans - The push for frequent upgrades contributes to a linear economy model, increasing demand for raw materials and waste generation. • Plastic and packaging waste - Mobile devices and accessories often come with excessive packaging, much of which is plastic and ends up in landfills or oceans. • Radiation and heat emissions - While typically low, large-scale deployment of mobile devices and towers may contribute to localised environmental heating and electromagnetic pollution. • Loss of biodiversity - Mining and manufacturing activities can lead to deforestation and ecosystem disruption, affecting wildlife and biodiversity. Accept any other valid response.	3		3

Question		Answer	AO1	AO2	Total
	(b)	*Describe the technology that allows for mobile phone communication.*			
		Indicative content Core Infrastructure • Cell towers (base stations): Enable coverage via "cells", receive and transmit signals to/from devices • Base station controllers (BSC): Manage multiple base stations, control resource allocation and handovers • Mobile Switching Centres (MSCs): Route voice calls/SMS, manage mobility and authentication • Backhaul infrastructure: Fibre optic and wired networks connect towers to the core network Transmission Technology • Radio Frequency (RF) Transmission: Mobile phones and towers communicate wirelessly using radio waves • Antennas: Used in both phones and towers to send and receive RF signals • SIM cards (Subscriber Identity Module): Securely store user identity and authorisation to connect to the network Network Technologies & Protocols • GSM / CDMA / LTE / 5G: Define how data is transmitted; each generation improves speed, bandwidth, and latency • Internet Protocol (IP)-based services: Used in 4G/5G for voice (VoIP), video calls, messaging, and internet access • Packet switching: Enables efficient data transfer in mobile internet services • Hardware components in relation to mobile technologies. Support Technologies • Handover (handoff): Maintains call/data continuity when users move between cells • Baseband processors: Chips in phones that manage signal processing (modulation, encoding) • Routers/switches: Move mobile data across the internet backbone • Data centres: Store and manage app/content delivery for mobile users (e.g. streaming, social media) Security and Authorisation • Encryption: Protects data in transit (calls, messages, internet) • SIM authentication: Verifies device and user for secure network access	8		8

Question	Answer	AO1	AO2	Total

Band	AO1
4	**7 – 8 marks** Excellent description which shows: • thorough knowledge and understanding of mobile phone communication • a confident grasp of how technology supports mobile phone communication.
3	**5 – 6 marks** Good description which shows: • generally secure knowledge and understanding of mobile phone communication • a generally secure grasp of how technology supports mobile phone communication.
2	**3 - 4 marks** Basic description which demonstrates: • some knowledge and understanding of mobile phone communication • some grasp of how technology supports mobile phone communication providers.
1	**1 - 2 marks** Limited description which demonstrates: • little knowledge and understanding of mobile phone communication • little grasp of how technology supports mobile phone communication
	0 marks • response not creditworthy or not attempted.

Question		Answer	AO1	AO2	Total
7	*(a)*	*A common form of social engineering is a phishing attack.* *Consider how this form of social engineering could be used to gain access and cause damage to a retail company's systems.*			
		Indicative content How access is gained: • Email deception: Fraudulent emails crafted to mimic trusted sources (e.g. internal departments, suppliers). • Credential harvesting: Victims are tricked into entering login details on fake portals. • Malicious attachments or links: Clicking may install malware or redirect to compromised websites. • Third-party exploitation: Attacks targeting suppliers or logistics partners to gain indirect access (supply chain attack). How damage is caused: • Information and systems o Data breach: Theft of customer data (e.g. emails, credit card details, addresses). o System access: Use of stolen credentials to infiltrate POS systems, inventory databases, or admin panels. o Intellectual property theft: Loss of confidential product designs, marketing plans, or pricing models. • Operations and finances o Service disruption: Systems disabled or infected with ransomware; downtime disrupts orders and payments. o Financial fraud: Redirected supplier payments, fraudulent purchases, or refund scams. o Reputational damage: Loss of customer trust, negative media coverage, and reduced brand loyalty.		6	6

Question	Answer	AO1	AO2	Total

Band	AO2
3	**5 – 6 marks** A very good consideration, which shows: • thorough knowledge and understanding of social engineering • a confident grasp of how this form of social engineering could be used to gain access to their system.
2	**3 - 4 marks** A good consideration, which shows: • generally secure knowledge and understanding of social engineering • a generally secure grasp of how this form of social engineering could be used to gain access to their system
1	**1 - 2 marks** A basic consideration, which shows: • some knowledge and understanding of social engineering • some grasp of how this form of social engineering could be used to gain access to their system
	0 marks • response not creditworthy or not attempted.

	(b)	*Discuss the legal frameworks that exist to protect against this form of social engineering*			
		Indicative content Data Protection Act 2018 and GDPR • These regulations impose stringent requirements for the protection of personal data • They require organisations to secure sensitive data, inform individuals of data breaches, and implement appropriate security measures • Fines can be imposed for non-compliance. Computer Misuse Act 1990 • This act criminalises unauthorised access to computer systems, including phishing attacks and other forms of cyber intrusion • Penalties for offenses under this act include fines and imprisonment. Fraud Act 2006 • The Fraud Act encompasses various fraudulent activities, including phishing, and sets out offenses related to fraud • It includes provisions for fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. • Penalties can include fines and imprisonment. Serious Crime Act 2015 • This act addresses computer misuse, including activities that may lead to unauthorised access, identity theft, and fraud. • It provides for criminal offenses and penalties for		6	6

Question		Answer	AO1	AO2	Total
		such activities. Investigatory Powers Act 2016 (RIPA) • This act grants law enforcement agencies the power to access and intercept electronic communications under certain circumstances • while providing safeguards to protect privacy rights. Financial Conduct Authority (FCA) Regulations • The FCA, as the financial regulatory authority, imposes requirements on financial institutions, including those related to cybersecurity and data protection. • Organisations in the finance sector must comply with these regulations to protect against financial cybercrimes. National Cyber Security Centre (NCSC) Guidance • The NCSC provides guidance and best practices for organisations to protect against cyber threats, including phishing attacks. • While not a legal framework, compliance with NCSC guidelines is strongly recommended. • Police and law enforcement agencies: They have investigative powers to address cybercrimes, including phishing attacks • can collaborate with other regulatory bodies to investigate and prosecute offenders.			

Band	AO2
3	**5 – 6 marks** A very good discussion, which shows: • thorough knowledge and understanding of legal frameworks • a confident grasp of legal frameworks that exist to protect against this form of social engineering.
2	**3 - 4 marks** A good discussion, which shows: • generally secure knowledge and understanding of legal frameworks • a generally secure grasp of legal frameworks that exist to protect against this form of social engineering
1	**1 - 2 marks** A basic discussion, which shows: • some knowledge and understanding of legal frameworks • some grasp of legal frameworks that exist to protect against this form of social engineering
	0 marks • response not creditworthy or not attempted.

Question		Answer	AO1	AO2	Total
8	*(a)*	*Give two characteristics each for VLAN and WLAN.*			
		Award two marks for each, up to a maximum of four marks **VLAN (MAX two marks):** • Logical segmentation of a physical network. • Logical segmentation of devices in a network. • Primarily used in wired networks. • Devices connected via wired Ethernet cables (Ethernet). • Segments a network for security, performance, or management. • Devices are grouped by VLAN IDs and connected to switches. • Devices in one VLAN are isolated from those in other VLANs. • VLANs in a corporate network separating finance, HR, and marketing departments. • Requires router for inter-VLAN communication. • VLANs provide traffic isolation and can be secured with access control lists (ACLs). **WLAN (MAX two marks):** • A network that allows wireless communication. • Physical medium (radio waves) for communication. • Primarily used in wireless networks. • Devices connect wirelessly via radio signals. • Provides mobility and flexibility by connecting devices wirelessly. • Devices connect to Access Points (APs). • Devices can roam across multiple access points in a WLAN. • A Wi-Fi network for wireless internet access. • No router needed for communication within the WLAN; router is needed for external internet access. • WLAN security relies on encryption protocols like WPA2 or WPA3. • Both are scalable.	2 2		4

Question		Answer	AO1	AO2	Total
	(b)	*Streaming platforms filter their content based on the user's geographical location. This is due to licensing agreements and regional restrictions.* *Consider the issues and implications for platforms and their response to the usage of VPN technologies with these platforms*			
		Indicative content Issue: • VPNs allow users to disguise or mask their real geographical location. • Users connect to a server in a different country to bypass regional restrictions (e.g. accessing U.S. Netflix content from the UK). • This can undermine licensing agreements that are based on country-specific content rights. Implications for Streaming Platforms • Revenue loss: Platforms or content creators may lose revenue due to users bypassing paid regional models. • Licensing violations: Platforms may breach contracts with distributors if users access region-locked content via VPNs. • Reputational damage: Users perceive unfairness (e.g. paying more for less content in their region). • Skewed analytics: VPN use distorts data about where users are located, affecting localisation, ads, and investment decisions. • Increased legal pressure: Platforms may face pressure from copyright holders to clamp down on location spoofing. Typical Platform Responses • VPN detection and blocking: Many platforms implement tech to detect and block VPN IP ranges (e.g. Netflix, BBC iPlayer). • Terms of service enforcement: Usage of VPNs to circumvent restrictions may violate user agreements. • Global licensing strategy: Some platforms (e.g. YouTube, Spotify) may shift towards making content globally accessible to reduce VPN pressure. • User notification or denial of service: Some platforms notify users that VPN use is detected and restrict access.		6	6

Question	Answer	AO1	AO2	Total

Band	AO2
3	**5 – 6 marks** A very good consideration, which shows: • thorough knowledge and understanding of VPN technologies • a confident grasp of the issues and implications for the provider **and** their response to the usage of VPN technologies with these platforms
2	**3 - 4 marks** A good consideration, which shows: • generally secure knowledge and understanding of VPN technologies • a generally secure grasp of the issues and implications for the provider **and/or** their response to the usage of VPN technologies with these platforms
1	**1 - 2 marks** A basic consideration, which shows: • some knowledge and understanding of VPN technologies • some grasp of the issues and implications for the provider **or** their response to the usage of VPN technologies with these platforms
	0 marks • response not creditworthy or not attempted.

Question	Answer	AO1	AO2	Total
9	*Discuss Cloud Computing services and how they benefit businesses*			

	Indicative content
	
	Cloud computing
	
	• Infrastructure as a Service (IaaS)
	  ○ Provides virtualised hardware resources such as servers, storage, and networks.
	• Platform as a Service (PaaS)
	  ○ Offers an environment for developing, testing, and deploying applications.
	• Software as a Service (SaaS)
	  ○ Delivers software applications via the internet on a subscription basis.
	• Function as a Service (FaaS) / Serverless Computing
	  ○ Executes code in response to events without server management.
	• Cloud Storage Services
	  ○ Supplies scalable, remote data storage that is easily accessible.
	• Cloud Backup and Disaster Recovery
	  ○ Ensures data backup and enables system restoration in case of failure.
	• Cloud Security Services
	  ○ Provides identity management, data protection, and threat monitoring in the cloud.
	• Content Delivery Networks (CDNs)
	  ○ Distributes digital content globally for faster access.
	• Cloud-Based Collaboration Tools
	  ○ Supports real-time communication and file sharing among teams.
	• Big Data and Analytics Services
	  ○ Offers platforms for processing and analysing large volumes of data.
	
	Business Benefits of Cloud Computing
	
	• Reduced Capital and Operational Costs
	  ○ Minimises the need for physical infrastructure and in-house maintenance.
	• Faster Development and Deployment
	  ○ Accelerates the creation and launch of applications.
	• Scalability and Flexibility
	  ○ Allows resources to be scaled up or down based on demand.
	• Remote Access and Mobility
	  ○ Enables employees to work and collaborate from anywhere.
	• Improved Business Continuity
	  ○ Protects against data loss and supports rapid disaster recovery.
	• Enhanced Security and Compliance
			10	10

Question	Answer	AO1	AO2	Total
	○ Offers built-in security tools and helps meet regulatory requirements. • Global Reach and Performance ○ Delivers content and services efficiently to users worldwide. • Data-Driven Decision Making ○ Empowers businesses to extract insights and trends from large datasets. • Pay-as-You-Go Pricing ○ Charges only for resources used, improving cost-efficiency. • Innovation Enablement ○ Frees up IT teams to focus on strategic initiatives rather than maintenance.			

Band	AO2
4	**9 – 10 marks** Excellent discussion which shows: • thorough knowledge and understanding of cloud computing services • a confident grasp of how cloud computing services benefits businesses
3	**6 – 8 marks** Good discussion which shows: • generally secure knowledge and understanding of cloud computing services • a generally secure grasp of how cloud computing services benefits businesses
2	**3 - 5 marks** Basic discussion which demonstrates: • some knowledge and understanding of cloud computing services • some grasp of how cloud computing provides services **and/or** benefits to businesses
1	**1 - 2 marks** Limited discussion which demonstrates: • little knowledge and understanding of cloud computing services • little grasp of how cloud computing provides services **or** benefits to businesses.
	0 marks • response not creditworthy or not attempted.