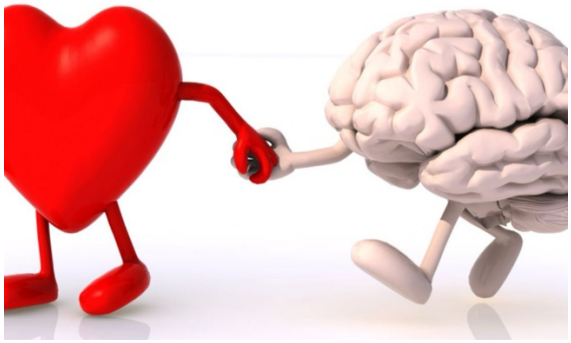
Newsome Academy

BTEC COMPUTING

DIGITAL INFORMATION TECHNOLOGY (DIT)

Cheat Sheet & Key Reminders for Fabulous Outcomes



MR WATKIN SUMMER 2025

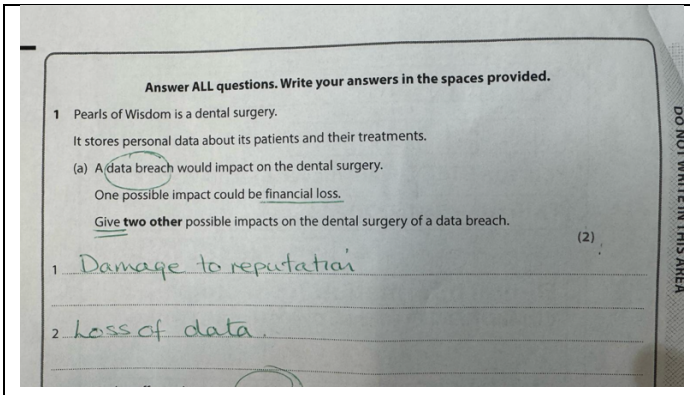
Types of Questions for Maximum Marks

The question and the marks should help you know how to answer each question. Remember what we have learnt in lessons in how you use **paragraphs** and **bullet-points** to make it easier for the examiner to give you marks.

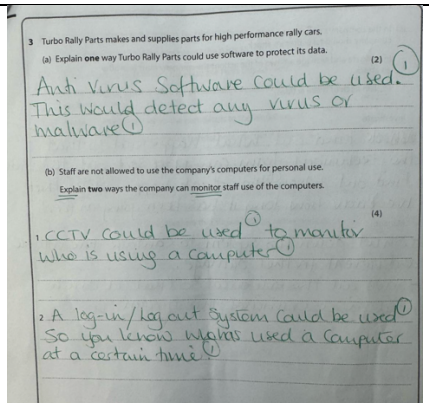
- **Give** - all you need to do is name or give simple responses.
- **Identify** – all you need to do is name or give simple responses.
- **State** - all you need to do is name or give simple responses.
- **Describe** – this requires and response and then an explanation/detail linking it to the topic.
- **Explain** - this requires and response and then an explanation/detail linking it to the topic.
- **Discuss** – more difficult but requires you to make decisions based on positives and negatives and give a well-rounded answer.
- **Evaluate** - more difficult but requires you to make decisions based on positives and negatives, give your view and give a well-rounded answer considering all factors.

Remember the marks awarded to the question should help you know how many paragraphs/bullet-points you should structure your writing in.

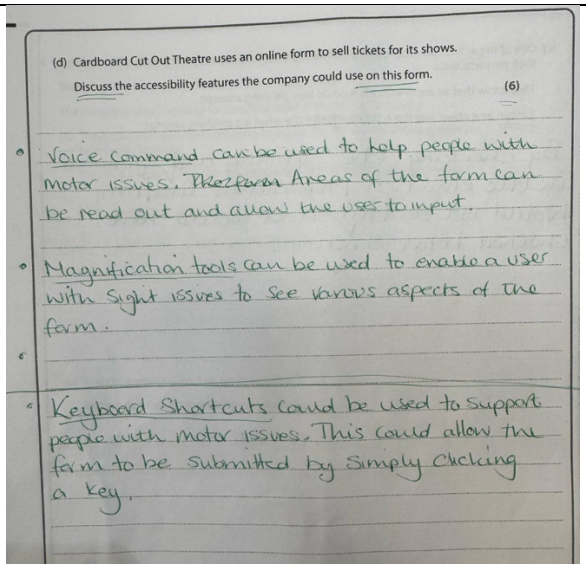
Examples

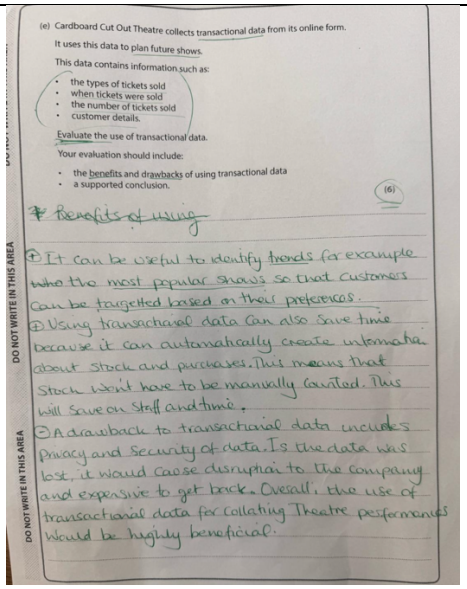


GIVE



EXPLAIN





Key Areas with Lost Marks from Mock Exam

Security – 2 factor security

Benefits of email

Cloud Computing

Monitoring software

Phishing

Transactional Data

Data Breaches & Cyber Attacks

BENEFITS OF EMAIL

Question 1:

What are the primary advantages of using email as a communication tool in a business environment?

Answer: The primary advantages of using email in a business environment include:

1. **Speed:** Emails can be sent and received almost instantaneously, facilitating quick communication.
2. **Cost-Effective:** Emailing reduces costs associated with traditional mail and long-distance communication.
3. **Documentation:** Emails provide a written record of communication, which can be useful for future reference or legal purposes.
4. **Accessibility:** Emails can be accessed from various devices, allowing employees to communicate from anywhere.
5. **Efficiency:** Bulk emailing allows for sending messages to multiple recipients simultaneously, saving time.

Question 2:

How does email enhance collaboration among team members?

Answer: Email enhances collaboration among team members by:

1. **Group Communication:** It enables group discussions and sharing of information among team members through distribution lists or cc/bcc options.
2. **File Sharing:** Emails allow the attachment of documents, images, and other files, making it easy to share resources.
3. **Asynchronous Communication:** Team members can respond at their convenience, accommodating different schedules and time zones.
4. **Integration with Other Tools:** Email can be integrated with project management tools, calendars, and other applications, streamlining workflow.

Question 3:

What are some security benefits of using email for business communication?

Answer: Security benefits of using email for business communication include:

1. **Encryption:** Emails can be encrypted to protect sensitive information from unauthorized access.
2. **Access Control:** Organizations can control who has access to email accounts and sensitive information.
3. **Auditing:** Email systems often include logging and monitoring features that help track communications for security audits.
4. **Anti-Virus and Anti-Phishing Tools:** Many email services provide built-in security measures to detect and filter out malicious content.

Question 4:

In what ways can email improve customer communication and service?

Answer: Email can improve customer communication and service by:

1. **Instant Acknowledgment:** Customers receive immediate confirmation of their inquiries or orders, enhancing their experience.

2. **Personalized Communication:** Businesses can personalize emails to address customer needs and preferences.
3. **Follow-Up Opportunities:** Automated follow-up emails can be sent to check on customer satisfaction or offer further assistance.
4. **Cost-Effective Marketing:** Email marketing campaigns can be targeted to specific customer segments, providing a cost-effective way to reach and engage customers.

Question 5:

What role does email play in project management?

Answer: Email plays a crucial role in project management by:

1. **Status Updates:** Project managers can send regular updates to stakeholders on project progress.
2. **Task Assignments:** Emails can be used to assign tasks to team members clearly and track responsibilities.
3. **Meeting Coordination:** Scheduling meetings and sharing agendas or minutes via email helps keep team members aligned.
4. **Feedback Loop:** Email provides a platform for feedback and suggestions, facilitating continuous improvement throughout the project lifecycle.

DATA SECURITY

Question 1:
What is data security, and why is it important in Digital Information Systems?
Answer: Data security involves protecting digital data from unauthorized access, corruption, theft, or damage. It is important because it ensures the confidentiality, integrity, and availability of data, helping organizations maintain trust, comply with laws, and prevent financial or reputational damage.

Question 2:
List and explain two common methods used to secure data.
Answer:

1. **Encryption:** Converts data into an unreadable format using algorithms, ensuring that only authorized parties with the decryption key can access the original information.
2. **Access Controls:** Restricts who can view or modify data by using authentication (like passwords or biometric verification) and permissions, ensuring only authorized users can access sensitive data.

Question 3:
What is multi-factor authentication (MFA), and how does it enhance data security?
Answer: Multi-factor authentication (MFA) requires users to verify their identity using two or more different methods, such as a password, a fingerprint, or a one-time code sent to a mobile device. It enhances data security by making it more difficult for unauthorized individuals to gain access, even if one factor (like a password) is compromised.

Question 4:
Describe two potential threats to data security.
Answer:

1. **Malware:** Malicious software such as viruses or ransomware that can damage, steal, or encrypt data, often leading to data loss or breaches.
2. **Phishing:** Fraudulent attempts to trick individuals into revealing sensitive information like passwords or financial details, which can then be used to access secure systems.

Question 5:
Why is regular data backup important for data security?
Answer: Regular data backup ensures that copies of important data are stored securely and can be restored in case of data loss due to hardware failure, cyberattacks, or accidents. It helps organizations recover quickly and reduces the impact of data breaches or system failures.

CLOUD COMPUTING

Question 1:
What is cloud computing, and what are its main characteristics?
Answer: Cloud computing is the delivery of computing services—including storage, processing power, and applications—over the internet. Its main characteristics include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured or pay-as-you-go service.

Question 2:
List and explain three advantages of using cloud computing for businesses.
Answer:

1. **Cost Savings:** Businesses can reduce expenses related to hardware, maintenance, and IT staff by using cloud services, paying only for what they use.
2. **Scalability:** Cloud resources can be scaled up or down quickly in response to demand, ensuring efficient use of resources.
3. **Accessibility:** Data and applications hosted in the cloud can be accessed from anywhere with an internet connection, supporting remote work and collaboration.

Question 3:
Identify and describe two potential risks associated with cloud computing.
Answer:

1. **Data Security and Privacy:** Storing sensitive data in the cloud raises concerns about unauthorized access, data breaches, and compliance with data protection regulations.
2. **Dependence on Service Providers:** Relying on third-party providers means that if they experience outages or go out of business, it can disrupt access to critical data and services.

Question 4:
What is a public cloud, and how does it differ from a private cloud?
Answer: A **public cloud** is a cloud environment where services are offered over the internet and shared among multiple organizations. Examples include Amazon Web Services (AWS) and Microsoft Azure.
A **private cloud** is a cloud infrastructure operated solely for a single organization, offering greater control and security but usually at higher costs. It can be hosted on-premises or by a third-party provider.

Question 5:
Explain what is meant by 'cloud service models' and name the three main types.
Answer: Cloud service models define the level of abstraction and services provided by cloud providers. The three main types are:

1. **Infrastructure as a Service (IaaS):** Provides virtualized hardware resources such as servers and storage.
2. **Platform as a Service (PaaS):** Offers a platform allowing customers to develop, run, and manage applications without managing underlying infrastructure.
3. **Software as a Service (SaaS):** Delivers software applications over the internet on a subscription basis, e.g., email services like Gmail.

DATA BREACHES

Question 1:
What is a data breach, and what are some common causes?
Answer: A data breach is an incident where sensitive, confidential, or protected data is accessed, disclosed, or stolen without authorization. Common causes include cyberattacks (such as hacking or malware), human error (like accidental sharing or misconfiguration), lost devices, or insider threats.

Question 2:
Describe two potential consequences of a data breach for an organization.
Answer:

1. **Loss of Trust and Reputation:** Customers and partners may lose confidence in the organization's ability to protect their data, leading to damage to its reputation.
2. **Legal and Financial Penalties:** Organizations may face fines, legal action, and increased regulatory scrutiny if they fail to protect data adequately, especially under laws like GDPR.

Question 3:
What measures can organizations take to prevent data breaches?
Answer: Organizations can implement strong security measures such as:

- Encryption of sensitive data
- Regular security updates and patches
- Employee training on cybersecurity best practices
- Multi-factor authentication
- Access controls and user permissions
- Regular security audits and vulnerability assessments

Question 4:
Explain how human error can lead to data breaches and give an example.
Answer: Human error can lead to data breaches when employees accidentally disclose or mishandle sensitive data. For example, sending an email containing confidential information to the wrong recipient or misconfiguring security settings on a cloud storage account can result in unauthorized access.

Question 5:
What role do regulations like GDPR play in preventing data breaches?
Answer: Regulations like the General Data Protection Regulation (GDPR) set legal requirements for organizations to protect personal data. They mandate data security measures, breach notification procedures, and penalties for non-compliance, encouraging organizations to implement robust security practices to prevent breaches.

MONITORING SOFTWARE

Question 1:

What is monitoring software, and what are its primary functions in an organizational context?

Answer: Monitoring software refers to applications designed to track and analyze user activities, system performance, and network security within an organization. Its primary functions include:

1. **Activity Tracking:** Monitoring user actions on devices to ensure compliance with organizational policies.
2. **Performance Monitoring:** Analyzing system performance metrics to identify bottlenecks or issues.
3. **Security Monitoring:** Detecting unauthorized access, malware, and other security threats in real-time.
4. **Data Analysis:** Providing insights into user behavior, application usage, and resource allocation.
5. **Reporting:** Generating reports to help management make informed decisions based on monitoring data.

Question 2:

What are the benefits of using monitoring software in an organization?

Answer: The benefits of using monitoring software include:

1. **Enhanced Security:** Provides real-time alerts and logs to prevent data breaches and cyberattacks.
2. **Increased Productivity:** Identifies unproductive behavior and areas where employees may need support or training.
3. **Compliance Assurance:** Helps ensure adherence to industry regulations and internal policies by tracking user activities.
4. **Resource Optimization:** Analyzes system usage to ensure that resources are allocated efficiently and effectively.
5. **Incident Response:** Facilitates rapid response to incidents by maintaining logs and records of user activities.

Question 3:

What types of monitoring software are commonly used in organizations, and what are their specific purposes?

Answer: Common types of monitoring software include:

1. **Network Monitoring Tools:** Monitor network traffic and performance to identify potential issues and optimize bandwidth.
2. **Employee Monitoring Software:** Tracks employee activities on company devices to assess productivity and compliance with policies.
3. **Application Performance Monitoring (APM):** Analyzes the performance of software applications to ensure they run efficiently and meet user expectations.
4. **Security Information and Event Management (SIEM):** Aggregates and analyzes security data from various sources to detect and respond to threats.
5. **Endpoint Monitoring Software:** Monitors endpoints (like computers and mobile devices) for security, performance, and compliance purposes.

Question 4:

What are the ethical considerations organizations should keep in mind when implementing monitoring software?

Answer: Ethical considerations include:

1. **Privacy:** Respecting employee privacy and ensuring that monitoring does not invade personal space or communications.
2. **Transparency:** Informing employees about what is being monitored and the reasons behind it, promoting trust.
3. **Consent:** Obtaining consent from employees where necessary, particularly in jurisdictions with strict privacy laws.
4. **Purpose Limitation:** Ensuring that monitoring is conducted for legitimate business purposes and not for intrusive surveillance.
5. **Data Protection:** Implementing measures to protect the data collected through monitoring software and ensuring it is not misused.

Question 5:

How can monitoring software aid in IT resource management within an organization?

Answer: Monitoring software aids in IT resource management by:

1. **Performance Insights:** Providing data on system performance, resource utilization, and application efficiency to inform decision-making.
2. **Capacity Planning:** Helping IT teams predict future resource needs based on usage trends and performance metrics.
3. **Cost Management:** Identifying underutilized resources or applications, allowing organizations to optimize costs and reduce waste.
4. **Troubleshooting:** Quickly identifying and resolving issues related to hardware or software, minimizing downtime and disruptions.
5. **Compliance Monitoring:** Ensuring that IT resources are used in accordance with company policies and regulatory requirements.

PHISHING

Question 1:

What is phishing, and how does it typically occur?

Answer: Phishing is a type of cyber attack where attackers impersonate legitimate organizations or individuals to deceive individuals into providing sensitive information, such as usernames, passwords, or financial details. It typically occurs through:

1. **Email:** Attackers send fraudulent emails that appear to be from reputable sources, prompting recipients to click on malicious links or download harmful attachments.
2. **Social Media:** Phishing can occur through direct messages or posts that appear to come from trusted contacts, often leading to fake websites.
3. **SMS (Smishing):** Phishing attempts can also be made via text messages, tricking users into providing personal information.
4. **Voice Phishing (Vishing):** Attackers may call individuals pretending to be from a legitimate organization and ask for sensitive information.

Question 2:

What are some common signs of a phishing attempt?

Answer: Common signs of a phishing attempt include:

1. **Suspicious Sender:** The email address may have slight variations from a legitimate source or be from a free email provider.
2. **Generic Greetings:** Phishing emails often use generic salutations like "Dear Customer" instead of personalizing the message.
3. **Urgent Language:** Messages that create a sense of urgency or panic, urging the recipient to act quickly, are often phishing attempts.
4. **Unusual Requests:** Requests for personal information, passwords, or payment details, especially through email, are red flags.
5. **Poor Grammar and Spelling:** Many phishing emails contain grammatical errors or awkward phrasing that indicates a lack of professionalism.

Question 3:

What are the potential consequences of falling for a phishing attack?

Answer: The potential consequences of falling for a phishing attack include:

1. **Identity Theft:** Attackers may gain access to personal information and use it to impersonate the victim or commit fraud.
2. **Financial Loss:** Victims may suffer financial losses through unauthorized transactions or theft of funds from bank accounts.
3. **Data Breaches:** Compromised accounts can lead to data breaches, affecting both individuals and organizations.
4. **Malware Infection:** Clicking on malicious links can result in the installation of malware, ransomware, or spyware on the victim's device.
5. **Reputation Damage:** For organizations, falling victim to phishing can damage their reputation and erode customer trust.

Question 4:

What measures can individuals and organizations take to protect themselves from phishing attacks?

Answer: Individuals and organizations can take several measures to protect themselves from phishing attacks, including:

1. **Education and Training:** Regularly training employees and individuals on recognizing phishing attempts and safe online practices.
2. **Email Filtering:** Implementing email filtering solutions to detect and block potential phishing emails before they reach users' inboxes.
3. **Multi-Factor Authentication (MFA):** Enabling MFA adds an extra layer of security, making it harder for attackers to access accounts even if credentials are compromised.
4. **Verification Practices:** Encouraging users to verify requests for sensitive information by contacting the organization directly through official channels.
5. **Regular Software Updates:** Keeping software and security systems updated to protect against known vulnerabilities that attackers may exploit.

Question 5:

How can organizations respond to a successful phishing attack?

Answer: Organizations can respond to a successful phishing attack by:

1. **Immediate Response:** Quickly isolating affected accounts or systems to prevent further damage and unauthorized access.
2. **Incident Reporting:** Documenting the incident and reporting it to relevant authorities, such as cybersecurity teams or law enforcement.
3. **User Notification:** Informing affected users about the breach, advising them on steps to secure their accounts and monitor for suspicious activity.
4. **Investigation:** Conducting a thorough investigation to understand how the attack occurred and identifying vulnerabilities that need to be addressed.
5. **Policy Review and Update:** Reviewing and updating security policies and training programs to prevent future incidents and enhance awareness.

TRANSACTIONAL DATA

Question 1:

What is transactional data, and why is it important for organizations?

Answer: Transactional data refers to the data generated from transactions or interactions within an organization, such as sales, purchases, payments, and customer interactions. It is important for organizations because it:

1. **Supports Decision-Making:** Provides insights into customer behavior, sales trends, and operational efficiency, enabling informed business decisions.
2. **Operational Efficiency:** Helps organizations streamline processes by analyzing transaction patterns and identifying areas for improvement.
3. **Customer Relationship Management:** Contains valuable information that can enhance customer relationships through targeted marketing and personalized services.
4. **Financial Reporting:** Forms the basis for financial records and statements, essential for compliance and performance evaluation.
5. **Data Analysis and Forecasting:** Enables organizations to conduct data analysis and forecasting to predict future trends and demands.

Question 2:

What are the key characteristics of transactional data?

Answer: Key characteristics of transactional data include:

1. **Time-Stamped:** Each transaction is recorded with a timestamp, indicating when it occurred.
2. **Detail-Oriented:** Contains detailed information about each transaction, such as product/service details, quantities, prices, and customer information.
3. **Volume:** Typically generated in high volumes, especially in organizations with frequent transactions.
4. **Structured Format:** Often structured in a specific format, such as rows and columns in a database, making it easier to store, retrieve, and analyze.
5. **Dynamic Nature:** Transactional data is continuously updated as new transactions occur, reflecting the most current state of business activities.

Question 3:

What are some common sources of transactional data in organizations?

Answer: Common sources of transactional data in organizations include:

1. **Point of Sale (POS) Systems:** Capture sales transactions at retail locations, including product details, prices, and payment methods.
2. **E-Commerce Platforms:** Generate data from online transactions, including customer purchases, returns, and shipping information.
3. **Customer Relationship Management (CRM) Systems:** Collect data on customer interactions, sales activities, and service requests.
4. **Financial Systems:** Record financial transactions, such as invoices, payments, and expense reports.
5. **Supply Chain Management Systems:** Track inventory movements, orders, and deliveries, providing data on procurement and logistics.

Question 4:

How can organizations utilize transactional data to improve customer experience?

Answer: Organizations can utilize transactional data to improve customer experience by:

1. **Personalization:** Analyzing purchase history allows for personalized recommendations and targeted marketing campaigns.
2. **Customer Insights:** Understanding customer preferences and behaviors helps tailor services and products to meet their needs.
3. **Feedback and Improvement:** Collecting data on customer interactions can identify areas for improvement in products or services.
4. **Loyalty Programs:** Analyzing transaction data can help design effective loyalty programs that reward repeat customers.
5. **Customer Support:** Access to transaction history enables customer support teams to provide informed assistance and resolve issues more efficiently.

Question 5:

What are some challenges associated with managing transactional data?

Answer: Challenges associated with managing transactional data include:

1. **Data Volume:** The high volume of data generated can overwhelm storage and processing capabilities, requiring robust data management solutions.
2. **Data Quality:** Ensuring the accuracy, consistency, and completeness of transactional data can be difficult, leading to potential errors in analysis.
3. **Integration:** Integrating transactional data from multiple sources or systems can be complex and may require significant resources and time.
4. **Security and Privacy:** Protecting sensitive transactional data from breaches while complying with data protection regulations is a significant concern.
5. **Real-Time Processing:** Organizations may struggle to process and analyze transactional data in real-time, which is essential for timely decision-making.