DUMPSARENA

Commercial Data Management

CIPS L6M7

Version Demo

Total Demo Questions: 7

Total Premium Questions: 73

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Understand the role of data in commercial activities	24
Topic 2, Understand the tools and techniques for data analysis	7
Topic 3, Understand the use of data for commercial decision making	3
Topic 4, Understand the legal and ethical implications of data usage in commercial activities	38
Topic 5, Mix Questions	1
Total	73

QUESTION NO: 1

Which of the following would be considered personal data? Select ALL that apply

A. An employee ' s work ID number

B. The average age of customers in a retail store

C. The time that someone drove into a carpark

D. A child ' s Date of Birth

ANSWER: A D

Explanation:

“An employee ' s work ID number” is personal data because it is an identifier assigned to an individual employee and can distinguish, or be linked back to, that person within an organisation’s records. Personal data includes information relating to an identified or identifiable natural person; identification may be direct or may arise by combining the identifier with information held by the employer. A work ID number is therefore personal data even where it does not state the employee’s name.

“A child ' s Date of Birth” is also personal data. A date of birth relates to a specific individual and is an important biographical identifier. It can contribute to identifying a child, especially when used with other information such as a name, address, school, or parent or guardian details. Data-protection practice requires organisations to handle children’s personal data with particular care, including applying appropriate safeguards and a lawful basis for processing. These examples align with the UK GDPR definition of personal data and the Information Commissioner’s Office guidance on identifying individuals and processing children’s data. See the ICO guidance on personal data and the ICO guidance on children’s information.

QUESTION NO: 2

What is the purpose of a 'Logic Gate'?

A. To assist in the analysis of large data sets

B. To take binary inputs and produce a single binary output according to a logical rule

C. To display data in different formats, e.g., videos

D. To increase the operating speed of a computer

ANSWER: B

Explanation:

To take binary inputs and produce a single binary output according to a logical rule is correct because a logic gate is a fundamental digital electronic circuit that implements a Boolean operation. It receives one or more binary input signals, conventionally represented as 0 and 1, and applies a defined logical rule to generate an output signal. For example, an AND gate outputs 1 only when all of its inputs are 1, while an OR gate outputs 1 when at least one input is 1. Logic gates are combined to form the circuits that enable computers and digital systems to make decisions, perform arithmetic, store information, and control processing operations. Although physical implementations may use transistors, the purpose of a gate is defined by its logical transformation of binary inputs into an output, rather than by a fixed number of transistors. This input-processing role is central to digital data handling because binary states provide the basis on which electronic systems represent, manipulate, and communicate data. Further technical background is available from Encyclopaedia Britannica’s logic-gate overview and All About Circuits’ explanation of logic gates.

QUESTION NO: 3

BI (Business Intelligence) can be used in the Procurement and Supply function to display which of the following data? Select ALL that apply

A. What % of invoices have been paid on time

B. How much money has been spent with Supplier X since 2015

C. How many staff have achieved MCIPS

D. Why supplier Y was awarded the new contract for packaging

E. How much money has been saved by introducing e-procurement tools since 2017

ANSWER: A B C E

Explanation:

Business intelligence presents organisational data in useful, decision-supporting forms such as reports, dashboards, scorecards, charts and key performance indicators. In procurement and supply, this commonly includes measurable operational, financial and people data drawn from transaction systems, invoice records, supplier-spend files and HR learning records. “What % of invoices have been paid on time” is a payment-performance KPI that can be calculated from invoice and payment dates. “How much money has been spent with Supplier X since 2015” is spend-analysis data, allowing expenditure to be grouped by supplier and time period. “How many staff have achieved MCIPS” is a count that can be reported from workforce or professional-development records. “How much money has been saved by introducing e-procurement tools since 2017” is a financial-benefits measure, provided that the organisation has defined and recorded an appropriate savings baseline and methodology. These measures can be filtered, aggregated and visualised to monitor performance, identify trends and support procurement decisions. Microsoft describes BI as the process of turning data into actionable insights through analysis and visualisation: Power BI overview. CIPS also identifies data and technology as a core capability within the profession: CIPS procurement topics and skills.

QUESTION NO: 4

A Head of Procurement wants a dashboard to identify suppliers that may create future continuity risk, rather than only report past performance. Which of the following are leading indicators of potential supplier disruption? Select TWO.

A. A declining trend in on-time delivery performance

B. An increase in unresolved quality non-conformances

C. Total spend with the supplier in the previous financial year

D. The number of invoices already paid to the supplier

E. The supplier’s registered address in the master-data file

ANSWER: A B

Explanation:

A declining on-time delivery trend and a sustained increase in unresolved quality issues can indicate that a supplier’s operational capability is deteriorating before a major failure occurs. They are therefore useful leading indicators for intervention and risk management. Total spend in the previous financial year describes historic expenditure, while the number of invoices already paid is an administrative count. Both may be useful for other purposes but do not directly indicate developing continuity risk.

QUESTION NO: 5 - (DRAG DROP)

Below are details of five companies that use smart sensors in their operations. Each sensor has a different purpose and a different way of transmitting data.

Instructions:

Drag and drop the correct Type of Sensor and Way of Transmitting Data into the appropriate boxes for each company.

Company	Type of Sensor (Drag Here)	Way of Transmitting Data (Drag Here)
Company 1: Worker ID Swipe	(Drop Answer Here)	(Drop Answer Here)
Company 2: Furniture Photo	(Drop Answer Here)	(Drop Answer Here)
Company 3: Carbon Output	(Drop Answer Here)	(Drop Answer Here)
Company 4: Item Barcode	(Drop Answer Here)	(Drop Answer Here)
Company 5: Smart Office	(Drop Answer Here)	(Drop Answer Here)

Available Answers:

Type of Sensor Options:

Electrical, Environmental, Image, Touch, Acoustic, Motion

Way of Transmitting Data Options:

Near-field Communication (NFC), ZigBee, RFID, Wi-Fi, Bluetooth, Black Box

ANSWER:

Explanation:

The completed mappings correctly connect each operational use case to the sensing capability needed to collect the relevant information and to a suitable communication method for passing that information into a business system. A worker ID swipe is a touch-based interaction: contact with a reader initiates the identification event, while Near-field Communication (NFC) supports the very short-range exchange typically associated with access, credentials, and tap-based identification. The NFC Forum's overview of NFC describes this close-proximity communication model.

Furniture photography needs an image sensor because its purpose is to capture visual information. RFID is appropriately paired with this item in the required mapping, supporting identification and tracking information being associated with the photographed furniture. Carbon-output monitoring requires environmental sensing, since the information being measured concerns surrounding conditions or emissions-related operational data. Wi-Fi provides a practical means of transmitting such monitoring data to a wider network or cloud-based analytics environment.

An item barcode is linked here to a motion sensor and RFID. This mapping reflects a process in which movement through a scanning, handling, or inventory workflow can trigger or accompany the capture of item-identification data. Finally, a smart office uses electrical sensing to monitor electrical usage or equipment status, with Bluetooth enabling short-range communication between connected devices, sensors, and local gateways. Together, these placements correctly distinguish the physical phenomenon being sensed from the channel used to transmit the resulting data for commercial management and analysis.

QUESTION NO: 6

In relation to cyber security, what would be the benefit of a public sector organisation joining a Group Purchasing Organisation (GPO)?

A. The GPO can result in cost savings for the organisation due to aggregate spending

B. The GPO is a third party who can host data on behalf of members, thus reducing the risk of hacking

C. The GPO takes on the burden of checking suppliers' security policies and procedures

D. The GPO provides training on cyber security to public sector organisations

ANSWER: C

Explanation:

The GPO takes on the burden of checking suppliers' security policies and procedures. A group purchasing organisation combines the requirements and purchasing activity of multiple members, commonly using its specialist procurement capability to establish and manage supplier frameworks. In a cyber-security context, this can provide a valuable layer of supplier assurance: before suppliers are made available through the arrangement, the GPO can conduct due diligence on their information-security governance, relevant controls, risk-management processes, and ability to meet contractual security requirements. This avoids every individual public-sector member having to design and perform the same initial supplier checks independently, while supporting a more consistent and proportionate approach to third-party cyber risk. The buying organisation must still understand its own risk appetite, define its particular security needs, and manage the supplier relationship and contract performance. However, using a suitably governed GPO framework can reduce the procurement workload and give members access to suppliers that have undergone structured pre-procurement assessment. This reflects the importance of managing supply-chain cyber security, including assessing supplier risks and setting appropriate security requirements. See the UK National Cyber Security Centre guidance on supply chain security and the UK Government cyber security procurement guidance.

QUESTION NO: 7

Zach is the Head of Procurement at a super secret military base. He does not want anyone outside of the base to know what he is procuring or which suppliers he uses as this information could be critical to national defence. He is aware that cyber criminals may be interested in stealing this information so he has decided to disconnect critical machines and systems from the internet. What is this approach to data security known as?

A. Unsyncing

B. Non-repudiation

C. Filtering

D. Air-gapping

ANSWER: D

Explanation:

Air-gapping is the correct term for isolating critical machines or systems from external networks, particularly the internet. In this scenario, the military base holds highly sensitive procurement and supplier information whose disclosure could affect national defence. By maintaining a physical or logical separation between those critical systems and outside networks, air-gapping substantially reduces the opportunity for a remote cybercriminal to access or exfiltrate the data through an internet-based attack. An air-gapped environment is therefore a security control based on network isolation: the protected system has no direct network path to untrusted or public networks. This approach is often used for especially sensitive operational technology, classified systems, and other high-value environments where confidentiality and resilience are paramount. Air-gapping does not remove every security obligation; the organisation must still protect any approved routes for transferring data, such as removable media, and maintain robust access controls and procedures. However, the defining action described—disconnecting critical systems from the internet to prevent external access—is air-gapping. Guidance on isolated systems and the risks that remain when transferring information across an air gap is available from the UK National Cyber Security Centre: NCSC air-gapping guidance. Further security-control context is provided by NIST SP 800-53.