WGU Cybersecurity-Architecture-and-Engineering D488 Practice Questions

Shared by Greene on 30-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A financial institution is concerned about a potential data breach due to employees accessing the company network using personal devices. They have decided to implement a bring your own device (BYOD) policy to mitigate the risk.

Which risk mitigation strategy will reduce the risk of a data breach in this scenario?

Options:

A- Blocking access to the company network from personal devices
B- Conducting regular security audits of the company network
C- Implementing a mobile device management (MDM) solution
D- Providing security awareness training for employees

Answer:

C

Explanation:

The correct answer is C --- Implementing a mobile device management (MDM) solution.

WGU Cybersecurity Architecture and Engineering (KFO1 / D488) describes that an MDM solution enables organizations to enforce security policies on personal devices, such as encryption, remote wipe capabilities, and application controls. MDM allows safe access to corporate resources while managing the inherent risks of BYOD environments.

Blocking access (A) contradicts the BYOD policy goal. Security audits (B) monitor but do not control personal devices. Awareness training (D) is important but does not enforce technical protections on devices.

Reference Extract from Study Guide:

'Mobile device management (MDM) solutions enforce security policies on employee-owned devices, ensuring compliance and reducing the risks associated with BYOD implementations.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Mobile Device Security

==========

Question 2

Question Type: MultipleChoice

How are IT and globalization related?

Options:

A- IT allows businesses to have a global reach.
B- IT allows businesses to reach global HIPAA compliance.
C- IT allows businesses to create tax havens for global companies.
D- IT allows businesses to create a global common gateway interface (CGI).

Answer:

A

Explanation:

Information Technology (IT) has revolutionized the way businesses operate, enabling them to reach global markets and audiences. IT facilitates communication, data exchange, and operational efficiency across borders, allowing companies to manage global operations and engage with international customers seamlessly. This global reach is a critical aspect of modern business strategies, driven by advancements in IT infrastructure and services.

Question 3

Question Type: MultipleChoice

What allows a user to query information from an online database with a web application without revealing what they are viewing?

Options:

A- Secure function evaluation (SFE)
B- Private function evaluation (PFE)
C- Homomorphic encryption
D- Private information retrieval (PIR)

Answer:

D

Explanation:

The correct answer is D --- Private information retrieval (PIR).

WGU Cybersecurity Architecture and Engineering (KFO1 / D488) explains that PIR allows users to query a database in such a way that the server cannot determine what information the user is retrieving. It protects user privacy while enabling database interaction.

SFE (A) involves computing a function without revealing inputs. PFE (B) is similar to SFE but focuses on functions. Homomorphic encryption (C) allows computation but not necessarily private querying.

Reference Extract from Study Guide:

'Private Information Retrieval (PIR) enables users to access database information without revealing the nature of the query to the server, preserving user privacy.'

Question 4

Question Type: MultipleChoice

What is the role of the CPU in a computing environment?

Choose 2 answers

Options:

A- Carrying out the instructions of a computer program
B- Storing data as it is being processed
C- Directing electrical current over the circuit board
D- Connecting components to the system unit
E- Containing an arithmetic logic unit (ALU) that performs arithmetic and logic operations

Answer:

A, E

Explanation:

TheCentral Processing Unit (CPU)is the primary component of a computer that performs most of the processing inside a computer.

Carrying out the instructions of a computer program: The CPU executes program instructions, which are the basic tasks that tell the computer what to do.

Containing an arithmetic logic unit (ALU): The ALU performs all arithmetic and logic operations, such as addition, subtraction, and comparison.

The CPU also manages data flow between the computer's other components.

It fetches instructions from memory, decodes them, and then executes them, which involves performing calculations and making decisions.

'Computer Organization and Design: The Hardware/Software Interface' by David A. Patterson and John L. Hennessy.

'Modern Processor Design: Fundamentals of Superscalar Processors' by John Paul Shen and Mikko H. Lipasti.

Question 5

Question Type: MultipleChoice

A company is concerned about the security of its users' passwords and is looking for a solution to ensure that user credentials are kept safe.

What is the best solution?

Options:

A- Object storage
B- Password policies
C- Removable storage
D- Hardware key manager

Answer:

B

Explanation:

The correct answer is B --- Password policies.

WGU Cybersecurity Architecture and Engineering (KFO1 / D488) emphasizes that strong password policies, including requirements for complexity, minimum length, expiration, and reuse restrictions, are essential for protecting user credentials from compromise.

Object storage (A) and removable storage (C) deal with data storage, not password management. Hardware key managers (D) manage cryptographic keys, not passwords directly.

Reference Extract from Study Guide:

'Implementing strong password policies enforces secure password practices among users, reducing the risk of credential compromise.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Identity and Access Management Controls

==========

Question 6

Question Type: MultipleChoice

The security team has been tasked with selecting a password complexity policy for the organization.

Which password complexity policy option should be recommended?

Options:

A- Twelve characters with no symbols or numbers
B- Sixteen characters with at least one letter, one number, and one symbol
C- Four characters with at least one letter or one number
D- Eight characters with no symbols or numbers

Answer:

B

Explanation:

The correct answer is B --- Sixteen characters with at least one letter, one number, and one symbol.

According to the WGU Cybersecurity Architecture and Engineering (KFO1 / D488) Study Guide, strong password policies must enforce a minimum length (preferably 12 to 16 characters) and

require complexity, including uppercase and lowercase letters, numbers, and special characters. Sixteen-character passwords that include varied character types greatly increase the difficulty for attackers using brute-force or dictionary attacks.

Options A, C, and D either lack complexity or have too few characters, making them vulnerable to attacks.

Reference Extract from Study Guide:

'A strong password should be at least 12--16 characters long and include a mix of uppercase letters, lowercase letters, numbers, and special characters to maximize resistance to brute-force attacks.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Identity and AccessManagement Concepts

==========

Question 7

Question Type: MultipleChoice

Which part of the Uniform Resource Locator (URL) identifies the server on which the web page can be found?

Options:

A- Resource path ID
B- Domain name
C- Protocol
D- IP address

Answer:

B

Explanation:

The domain name in a Uniform Resource Locator (URL) identifies the server on which the web page can be found.

Example: In the URL 'http://www.example.com/index.html':

'http' is the protocol.

'www.example.com' is the domain name.

'/index.html' is the resource path ID.

The other options:

The protocol specifies the communication method.

The resource path ID specifies the specific page or resource on the server.

The IP address is not typically visible in the URL itself but can be resolved via DNS.

Therefore, the domain name is the correct part that identifies the server.

'Web Development and Design Foundations with HTML5' by Terry Felke-Morris, which explains URL components.

'Internet and World Wide Web How to Program' by Paul Deitel and Harvey Deitel, which covers URLs and their structure.

Question 8

Question Type: MultipleChoice

A company wants to improve the security of its software development process and reduce the risk of vulnerabilities in its applications. The company is looking for a solution that can isolate its applications and provide a secure environment for development and testing.

Which security technology meets the needs of this company?

Options:

A- Data loss prevention (DLP)
B- Virtual private network (VPN)
C- Firewall
D- Containerization

Answer:

D

Explanation:

The correct answer is D --- Containerization.

WGU Cybersecurity Architecture and Engineering (KFO1 / D488) material states that containerization provides isolated environments (containers) where applications can be developed, tested, and deployed securely. This isolation minimizes the risk of vulnerabilities affecting the host system or other applications, improving the overall security of the development process.

DLP (A) prevents data leakage but does not isolate applications. VPNs (B) secure network traffic but do not create isolated development environments. Firewalls (C) control network traffic but do not manage application-level isolation.

Reference Extract from Study Guide:

'Containerization secures application development and deployment by isolating applications in lightweight, standalone environments, reducing risk and improving manageability.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Application Security Concepts

==========

Question 9

Question Type: MultipleChoice

A security analyst for a financial institution is in the process of planning to upgrade the institution's IT infrastructure to meet current industry standards. There are various potential risks associated with the upgrade, including data breaches, system outages, and cost overruns. The analyst is tasked with managing these risks to ensure a successful upgrade.

What is the first step in the risk management life cycle in this scenario?

Options:

A- Assess
B- Control
C- Review
D- Identify

Answer:

D

Explanation:

The correct answer is D --- Identify.

According to WGU Cybersecurity Architecture and Engineering (KFO1 / D488), the first step in risk management is identifying potential risks. Only once risks are identified can they be assessed, controlled, and reviewed. In this case, identifying potential data breaches, outages, and cost issues is the starting point.

Assess (A) happens after identification. Control (B) involves implementing responses. Review (C) happens later to check effectiveness.

Reference Extract from Study Guide:

'The first phase of risk management is risk identification, where potential threats and vulnerabilities are recognized and documented.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Risk Management Life Cycle

==========

Question 10

Question Type: MultipleChoice

A government agency is required to comply with the Federal Information Security Modernization Act (FISMA), which establishes security requirements for federal information systems. The agency needs to secure its external network, which connects to the internet and is used by employees, contractors, and other authorized personnel.

Which security control will secure the external network and protect against unauthorized access?

Options:

A- Intrusion detection and prevention
B- Firewall
C- Access controls
D- Network segmentation

Answer:

B

Explanation:

The correct answer is B --- Firewall.

According to WGU Cybersecurity Architecture and Engineering (KFO1 / D488), firewalls are critical for securing external network perimeters by filtering incoming and outgoing traffic based on predefined security rules. This control is a foundational requirement under FISMA to prevent unauthorized access.

IDS/IPS (A) monitor and detect attacks but are secondary to establishing the initial network boundary. Access controls (C) manage user permissions inside a system. Network segmentation (D) divides internal networks but does not protect the external boundary.

Reference Extract from Study Guide:

'Firewalls are the first line of defense for securing external networks, providing traffic filtering to prevent unauthorized access, aligning with FISMA compliance requirements.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Network Security Fundamentals

==========

Question 11

Question Type: MultipleChoice

A professional services organization deployed security edge devices in key locations on its corporate network.

How will these devices improve the organization's security posture?

Options:

A- They act as an initial defense layer for potential threats
B- They protect from severe distributed denial-of-service (DDoS) attacks
C- They act as a security information and event management (SIEM) module for a security operations center (SOC) analyst
D- They are a set of trusted platform module (TPM) devices

Answer:

A

Explanation:

The correct answer is A --- They act as an initial defense layer for potential threats.

According to WGU Cybersecurity Architecture and Engineering (KFO1 / D488), security edge devices such as firewalls, secure web gateways, and intrusion prevention systems (IPS) are placed at the network perimeter to serve as the first layer of defense against external threats.

DDoS protection (B) may be part of a broader security solution but is not the main role of general edge devices. SIEM modules (C) collect and correlate logs, not defend at the perimeter. TPM devices (D) are hardware-based cryptographic modules, not network edge defenses.

Reference Extract from Study Guide:

'Security edge devices provide the first line of defense against external threats by monitoring, filtering, and blocking malicious traffic entering the corporate network.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Network Security and Perimeter Defense

Question 12

Question Type: MultipleChoice

An IT team has been tasked with improving the security of a company's web applications.

Which threats should the IT team consider detecting when defending the network with a web application firewall (WAF)?

Options:

A- Phishing attacks
B- Brute force attacks
C- Structured Query Language (SQL) injection attacks
D- Social engineering attacks

Answer:

C

Explanation:

The correct answer is C --- Structured Query Language (SQL) injection attacks.

As per WGU Cybersecurity Architecture and Engineering (KFO1 / D488), a Web Application Firewall (WAF) protects web applications by filtering and monitoring HTTP traffic. It isspecifically effective against attacks such as SQL injection, cross-site scripting (XSS), and other application-layer vulnerabilities.

Phishing (A) and social engineering (D) involve human deception, not web application vulnerabilities. Brute force attacks (B) typically target authentication but are not the primary focus of a WAF.

Reference Extract from Study Guide:

'A web application firewall (WAF) detects and prevents attacks against web applications, including SQL injection and cross-site scripting (XSS).'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Web Application Firewall and Threat Protection

==========

Question 13

Question Type: MultipleChoice

An e-learning company uses Amazon Simple Storage Service (Amazon S3) to store e-books and video files that are served to customers through a custom application. The company has realized that someone has been stealing its intellectual property.

Which threat actor is most likely in this scenario?

Options:

A- Advanced persistent threat
B- Novice hacker
C- Competitor
D- Hacktivist

Answer:

C

Explanation:

The correct answer is C --- Competitor.

According to WGU Cybersecurity Architecture and Engineering (KFO1 / D488), competitors often attempt to steal intellectual property to gain a business advantage. Given the theft of valuable business assets (e-books and videos), the most likely actor is a competitor motivated by financial or market advantage, not ideology or random hacking.

An APT (A) is usually nation-state-sponsored and targets critical infrastructure. A novice hacker (B) might deface or cause damage but is less likely focused on IP theft. Hacktivists (D) are politically motivated, not financially.

Reference Extract from Study Guide:

'Competitors may engage in cyber espionage to steal intellectual property and gain market advantage, representing a significant threat to business assets.'

--- WGU Cybersecurity Architecture and Engineering (KFO1 / D488), Threat Actor Categories

P2P exams

P2P exams

To Get Premium Files for Cybersecurity-Architecture-and-Engineering Visit

https://www.p2pexams.com/products/cybersecurity-architecture-and-engineering

For More Free Questions Visit

https://www.p2pexams.com/wgu/pdf/cybersecurity-architecture-and-engineering

