DUMPSBOSS.

# WGU Cybersecurity Architecture and Engineering (D488)

## WGU Cybersecurity-Architecture-and-Engineering

**Version Demo**

**Total Demo Questions: 23**

**Total Premium Questions: 235**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A security team is investigating multiple man-in-the-middle (MITM) attacks that have taken place on the corporate network over the past few months. The team needs a solution that will ensure that data is not exposed if a man-in-the-middle attack occurs in the future.

**A.** Enforcing password history

**B.** Encrypting data

**C.** Ensuring all users have complex passwords

**D.** Disabling Wi-Fi connections

**ANSWER: B**

**Explanation:**

Encrypting data is the appropriate control because it protects the confidentiality of information in transit even when an attacker is able to intercept network communications. When strong, properly configured transport encryption is used—such as TLS with valid certificate validation—the intercepted payload is encrypted and cannot be practically read without the required cryptographic keys. TLS also provides endpoint authentication and integrity protections that help the communicating parties detect attempts to alter traffic or impersonate a legitimate endpoint, both of which are central risks in a man-in-the-middle attack.

The protection depends on correct implementation: systems should use current TLS versions and strong cipher suites, validate the full certificate chain and hostname, and prevent users or applications from bypassing certificate warnings. Sensitive internal services should also use encrypted protocols rather than cleartext alternatives, so protection remains consistent across the corporate network. NIST guidance describes TLS as a mechanism for protecting the confidentiality and integrity of data exchanged over networks. See NIST SP 800-52 Rev. 2 and the NSA guidance on strong TLS configuration.

**QUESTION NO: 2**

What are two differences between a handheld computer and a desktop?

Choose 2 answers.

**A.** A handheld has more memory.

**B.** A desktop has more memory.

**C.** A desktop has more internal storage.

**D.** A handheld has more internal storage.

**ANSWER: B C**

**Explanation:**

A desktop has more memory and a desktop has more internal storage are generally valid distinctions in standard endpoint-hardware comparisons. Desktop computers are designed around larger chassis, continuous AC power, and easily serviceable components. Those characteristics allow manufacturers and users to install substantially more RAM, often across multiple memory slots, supporting demanding workloads such as virtualization, engineering software, large data sets, and extensive multitasking. Desktop platforms also commonly accommodate several internal storage devices, including multiple solid-state drives or hard disk drives, providing higher aggregate local capacity and flexible expansion. Handheld computers prioritize a small, lightweight, battery-powered form factor, so their memory and built-in storage are typically constrained by physical space, power consumption, thermal limits, and integrated hardware design. Although individual modern handheld models can have considerable capacity, the question asks for general differences rather than an absolute rule for every product. CompTIA's hardware overview describes desktop systems as modular and upgradeable, while its mobile-device material emphasizes compact, integrated mobile hardware. See CompTIA's desktop-computer guide and CompTIA's mobile-device guide.

## QUESTION NO: 3

A company is developing a new mobile application to support external customers and contractors. The application needs to allow users to sign in using third-party social identities.

What is the best protocol?

**A.** Security Assertion Markup Language (SAML)

**B.** Kerberos

**C.** Lightweight Directory Access Protocol (LDAP)

**D.** Open Authorization (OAuth)

**E.** OpenID Connect (OIDC)

## ANSWER: E

**Explanation:**

OpenID Connect (OIDC) is the best protocol because the requirement is to authenticate external users with identities managed by third-party social identity providers. OIDC is an identity layer built on OAuth 2.0 that enables a mobile application to request and validate standardized identity information about the signed-in user. After a user authenticates with a provider such as Google, Apple, or Microsoft, the application receives an ID token containing claims such as the user's unique identifier, name, and email address. The application validates the token's signature, issuer, audience, expiration, and nonce before establishing its own authenticated session. This provides a standards-based federated sign-in experience without requiring the company to create, store, or manage a separate password for every external customer or contractor. OIDC is designed for modern web and native mobile application sign-in flows and supports protections appropriate to public clients, including authorization code flow with Proof Key for Code Exchange (PKCE). OAuth 2.0 is the underlying delegated-authorization framework, but OIDC specifically supplies the authentication and identity-token semantics needed for "Sign in with" social identity scenarios. See the OpenID Foundation's OIDC overview and OpenID Connect Core 1.0.

## QUESTION NO: 4

The security team has been notified about multiple man-in-the-middle (MITM) attacks happening on the wireless network over the past thirty days. Management has agreed to upgrade the network infrastructure to help eliminate these attacks.

**A.** Security information and event management (SIEM)

**B.** Inline network encryptor

**C.** Layer 3 switch

**D.** Wireless intrusion prevention system (WIPS)

## ANSWER: D

**Explanation:**

Wireless intrusion prevention system (WIPS) is the appropriate infrastructure upgrade because it is purpose-built to identify, analyze, and actively respond to threats operating in the wireless radio-frequency environment. Wireless MITM activity commonly involves rogue access points, evil-twin access points impersonating a legitimate SSID, unauthorized associations, and suspicious wireless-management behavior. A WIPS uses dedicated sensors or access-point radio capabilities to continuously monitor the airspace, correlate observed devices and access points with the authorized wireless inventory, and alert or take configured containment actions when it identifies an unauthorized or malicious wireless device.

This provides controls at the point where the attacks occur: the wireless network itself. In addition to detecting rogue and evil-twin infrastructure, a well-configured WIPS supports ongoing visibility into wireless clients, access points, channels, and policy violations, allowing the security team to investigate repeated incidents and tune protective controls. NIST's wireless LAN guidance describes wireless intrusion detection and prevention capabilities as important mechanisms for identifying and

responding to wireless attacks and unauthorized wireless devices. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks and CISA guidance on evil-twin Wi-Fi attacks.

## QUESTION NO: 5

A security architect is designing protection for administrative access to production cloud resources. The organization wants to reduce the risk from long-lived privileged credentials and ensure that elevated access can be reviewed after use.

Which two controls should be implemented? Choose 2 answers.

**A.** Implement just-in-time privileged access with time-limited elevation

**B.** Use shared administrator accounts for operational continuity

**C.** Record and centrally retain privileged session activity

**D.** Assign permanent administrator roles to all infrastructure engineers

**E.** Store administrative passwords in deployment scripts

## ANSWER: A C

**Explanation:**

Just-in-time privileged access and centralized logging of privileged sessions directly address the stated requirements. Just-in-time access grants elevated permissions only when a user has an approved, time-limited business need. This reduces the exposure created by standing administrative privileges. Logging privileged sessions provides evidence for accountability, investigation, and post-access review.

Shared administrator accounts reduce accountability because activity cannot be reliably attributed to an individual. Permanent administrator membership creates long-lived elevated access rather than limiting it. Storing administrative passwords in deployment scripts exposes credentials and does not provide controlled, auditable privilege elevation.

## QUESTION NO: 6

What are three operating systems that are commonly used today?

Choose 3 answers

**A.** Microsoft Outlook

**B.** Mac OS

**C.** Linux

**D.** MySQL

**E.** Microsoft Windows

**F.** Mozilla Firefox

## ANSWER: B C E

**Explanation:**

Mac OS, more commonly branded as macOS, Linux, and Microsoft Windows are operating systems: foundational system software that manages a computer's hardware resources and provides the platform on which applications run. macOS is Apple's desktop operating system for Mac computers and supplies core services such as file management, process execution, memory management, user authentication, networking, and graphical user interaction. Apple documents macOS as the operating system powering Mac devices in its macOS overview.

Linux refers to a family of operating systems built around the Linux kernel and distributed in many forms, including Ubuntu, Red Hat Enterprise Linux, Debian, and Kali Linux. It is extensively used for servers, cloud workloads, embedded systems, security tools, and desktop computing. The Linux Foundation describes the kernel and its role in its What is Linux? resource. Microsoft Windows is Microsoft's widely deployed operating system family for consumer and enterprise endpoints; it provides the system environment, security controls, hardware support, and application services required to operate PCs. These three selections therefore fit the defining role of an operating system rather than being individual end-user applications or a database product.

## QUESTION NO: 7

A small online retailer stores customer information, product inventory, and financial data on its local servers.

What are the necessary components of a business continuity and disaster recovery plan for this company?

**A.** A detailed evacuation plan, frequent data backups, and regular cybersecurity training for employees

**B.** Redundant backups, a communication plan, and a designated off-site location for data storage and recovery

**C.** A comprehensive insurance policy, a list of emergency contacts, and a system for continuous monitoring of network activity

**D.** Routine maintenance of servers, an emergency generator, and a policy for employees to work remotely in case of a disaster

## ANSWER: B

**Explanation:**

Redundant backups, a communication plan, and a designated off-site location for data storage and recovery are necessary core components because they address the ability to restore critical systems and coordinate the organization's response after a disruptive event. Redundant backups protect the retailer's customer, inventory, and financial records against loss or corruption, while maintaining copies away from the primary site prevents a local incident—such as fire, flood, theft, or ransomware—from destroying both production systems and recoverable data. The recovery location can be a cloud-based environment, a colocation site, or another suitable alternate facility, provided it supports restoration within the business's recovery objectives.

A documented communication plan establishes who declares an incident, who performs recovery tasks, how personnel and vendors are contacted, and how the business communicates operational status to customers and other stakeholders. Together, these measures support both disaster recovery, which focuses on restoring technology and data, and business continuity, which focuses on sustaining or resuming essential operations at an acceptable level. Plans should also be tested regularly so backup restoration procedures, contact information, responsibilities, and recovery timing are validated rather than assumed. NIST describes contingency planning as preparing for system recovery and reconstitution following disruptions, including alternate processing and backup capabilities. See NIST SP 800-34 Rev. 1 and Ready.gov Business Continuity Planning Suite.

## QUESTION NO: 8

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)?

**A.** Phishing attacks

**B.** Brute force attacks

**C.** Structured Query Language (SQL) injection attacks

**D.** Social engineering attacks

## ANSWER: C

**Explanation:**

Structured Query Language (SQL) injection attacks are a core threat that a web application firewall (WAF) is designed to detect and help prevent. SQL injection occurs when an attacker supplies malicious SQL syntax through an application input, such as a login form, search field, URL parameter, or API request. If the application improperly incorporates that input into a database query, the attacker may be able to read, alter, or delete sensitive data, bypass authentication, or execute unintended database operations.

A WAF operates at the application layer and inspects HTTP/HTTPS requests and responses using rules, signatures, protocol validation, and behavioral techniques. This lets it identify common SQL injection indicators, including suspicious query operators, malformed input patterns, encoded payloads, and known attack signatures, before requests reach the web application or its database. WAF protections are especially valuable as a compensating or defense-in-depth control while development teams implement secure coding practices such as parameterized queries and server-side input validation.

SQL injection is recognized as a major web application security risk by the OWASP Top 10. The NIST definition of a web application firewall likewise describes a WAF as a firewall that protects web applications by applying rules to HTTP traffic.

## QUESTION NO: 9

A DevSecOps team is preparing a release of a web application that stores customer account information. The team wants to reduce the likelihood that known vulnerable third-party libraries or exposed secrets will reach production.

Which two controls should be integrated into the CI/CD pipeline? Choose 2 answers.

**A.** Perform software composition analysis on third-party dependencies

**B.** Disable dependency updates after the first successful build

**C.** Scan source code and build artifacts for exposed secrets

**D.** Store production credentials in the source-code repository

**E.** Delay security testing until after production deployment

## ANSWER: A C

**Explanation:**

Software composition analysis and secret scanning are the correct controls. Software composition analysis identifies third-party components and compares their versions against known vulnerability information, helping the team remediate or replace risky dependencies before release. Secret scanning detects credentials, API keys, tokens, and similar sensitive values that may have been accidentally committed to source code or build artifacts.

Disabling dependency updates leaves known vulnerable components in the application. Storing production credentials in source-code repositories exposes high-value secrets and makes rotation more difficult. Delaying security testing until after production deployment fails to prevent vulnerable libraries or exposed secrets from reaching the production environment.

## QUESTION NO: 10

An organization uses third-party contractors to administer network devices. The organization must prevent direct internet access to device-management interfaces and ensure that each administrative session is attributable to an individual contractor.

Which two controls should be implemented?

Choose 2 answers.

**A.** Require multifactor authentication for individual contractor accounts

**B.** Use a hardened bastion host for administrative connections

**C.** Provide all contractors with a shared administrator account

**D.** Expose Secure Shell management interfaces directly to the internet

**E.** Rely only on source IP address allowlisting for administrator access

**ANSWER: A B**

**Explanation:**

A hardened bastion host provides a controlled administrative entry point rather than exposing router, switch, and firewall management interfaces directly to the internet. Administrative sessions can be proxied through the bastion host and centrally logged for review.

Multifactor authentication tied to individual contractor accounts strengthens identity assurance and preserves accountability. A shared administrator account prevents reliable attribution, while source IP allowlisting alone does not establish the identity of the person using an allowed address. Exposing Secure Shell directly to the internet unnecessarily increases the attack surface.

## QUESTION NO: 11

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?

**A.** Advanced persistent threat

**B.** Novice hacker

**C.** Competitor

**D.** Hacktivist

**ANSWER: C**

**Explanation:**

**Competitor** is the most likely threat actor because the stated target is intellectual property: proprietary e-books and video content that has direct commercial value. A competing organization could benefit from acquiring that content without paying to create or license it, using it to accelerate its own offerings, reduce development costs, or gain market share. This is consistent with economic espionage and theft of trade secrets, in which proprietary business information is targeted for an economic advantage. The FBI describes economic espionage as theft or misappropriation of trade secrets intended to benefit a foreign government, instrumentality, or agent, and recognizes that theft of proprietary information harms a company's competitiveness. Although the scenario does not establish the specific technical path used to obtain the files, the actor's apparent motivation is the key indicator: stealing monetizable educational assets points to a business-driven adversary. Because the content is stored in Amazon S3 and delivered through an application, the organization should also protect against unauthorized retrieval by applying least-privilege access, blocking public access unless explicitly required, and monitoring access activity. AWS provides specific guidance for securing S3 data and access controls. See the FBI economic espionage overview and AWS S3 security best practices.

## QUESTION NO: 12

A software company is reviewing its disaster recovery plan and wants to identify the criticality of its business processes to prioritize its recovery efforts.

Which will determine the criticality of its business processes?

**A.** Business continuity planning (BCP)

**B.** Business impact analysis (BIA)

**C.** Disaster recovery (DR)

**D.** Incident response (IR)

**ANSWER: B**

**Explanation:**

Business impact analysis (BIA) determines the criticality of business processes by systematically identifying essential functions and evaluating the operational, financial, legal, reputational, and customer-service consequences if each function is disrupted. This analysis establishes which processes require the fastest restoration and provides measurable recovery requirements, such as recovery time objectives (RTOs) and recovery point objectives (RPOs). For example, a company may determine that customer authentication, payment processing, and source-code repositories have substantially different interruption impacts and therefore need different recovery priorities and resources.

A BIA is a core input to both business continuity and disaster recovery planning because recovery strategies must be aligned to the organization's actual business needs, dependencies, and maximum tolerable downtime. By documenting the impacts of outages over time, decision-makers can direct recovery investments toward the processes whose loss would cause the greatest harm. This makes Business impact analysis (BIA) the appropriate method for determining process criticality before finalizing recovery priorities. Guidance on conducting BIAs and using their results for continuity planning is available from Ready.gov and NIST SP 800-34 Rev. 1.

**QUESTION NO: 13**

A security operations center is establishing centralized log management for systems that process sensitive customer information. The organization must be able to investigate incidents using reliable records and detect unauthorized modification or deletion of collected logs.

Which two design decisions will best support these requirements? Choose 2 answers.

**A.** Send logs to a centralized platform using authenticated, encrypted transport

**B.** Allow administrators to alter local logs before forwarding them

**C.** Restrict log modification and deletion through role-based access control

**D.** Use one shared service account for all log-management functions

**E.** Disable time synchronization on systems that forward logs

**ANSWER: A C**

**Explanation:**

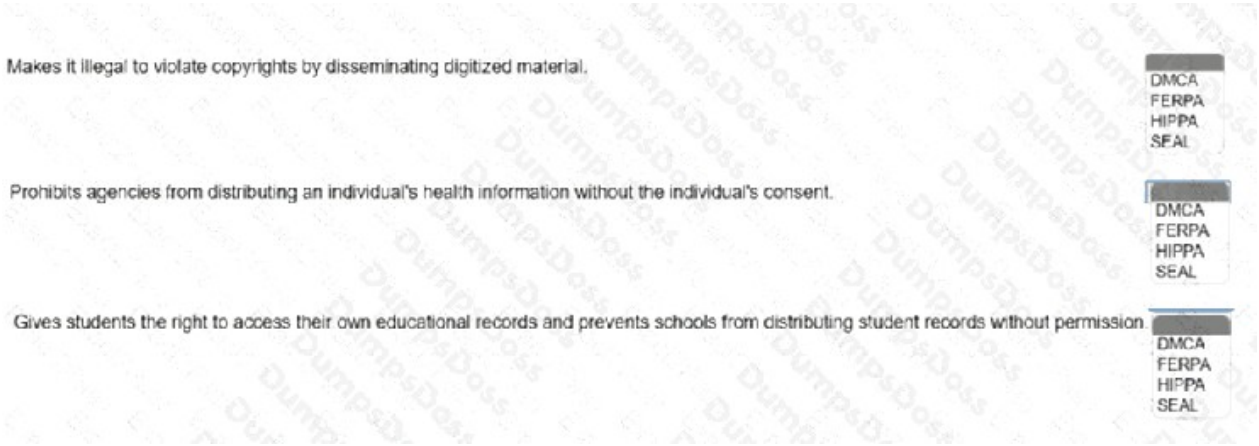
Sending logs to a centralized platform using authenticated, encrypted transport protects log records while they are transmitted and enables cross-system investigation. Restricting modification and deletion through role-based access control supports log integrity by ensuring that only explicitly authorized personnel and processes can manage retained records.

Allowing each administrator to alter local logs prevents reliable centralized investigation and weakens accountability. Reusing a shared service account makes it difficult to attribute actions. Disabling time synchronization makes correlation across systems unreliable because event timestamps cannot be accurately compared.

**QUESTION NO: 14 - (SIMULATION)**

Match the legislative purpose with the corresponding legislation.

Answer options may be used more than once or not at all.




**ANSWER: Check the explanation for the answer**

**Explanation:**

Match the purposes as follows:

DMCA protects digital copyrighted works; HIPAA protects protected health information (PHI); and FERPA protects student education records.

## QUESTION NO: 15

An organization is deploying a containerized application that processes internal financial data. The security team must reduce the container attack surface and limit the impact if an application process is compromised.

Which two container-hardening practices should be implemented?

Choose 2 answers.

**A.** Use a minimal, maintained base image

**B.** Run the application process as a non-root user

**C.** Run each container in privileged mode

**D.** Deploy images by using only a latest tag

**E.** Disable seccomp restrictions for all containers

**ANSWER: A B**

**Explanation:**

Using a minimal, maintained base image reduces the number of installed packages, libraries, and utilities that could contain vulnerabilities or be abused after compromise. Running the application as a non-root user limits the privileges available to a compromised process and supports least privilege.

Privileged containers weaken isolation by granting broad host-level capabilities. Using mutable latest tags undermines repeatable deployments and makes it difficult to determine which image version was deployed. Disabling security controls such as seccomp expands rather than reduces the container's available attack surface.

## QUESTION NO: 16

A company has recently experienced a data breach in which customer information was stolen. The company is concerned about the potential for future data breaches. A review of the incident revealed that the breach originated from stolen credentials.

Which security measure will meet the needs of this company?

**A.** Implementing two-factor authentication

**B.** Conducting background checks on employees

**C.** Providing regular security awareness training to employees

**D.** Installing a security information and event management (SIEM) system

**ANSWER: A**

**Explanation:**

Implementing two-factor authentication is the appropriate measure because the incident originated with stolen credentials. Two-factor authentication requires a user to supply a second, independent authentication factor in addition to a password, such as a cryptographic security key, an authenticator-app code, or a biometric factor. Consequently, possession of a stolen password alone is insufficient to authenticate as the affected user. This directly reduces the likelihood that compromised credentials can be reused to gain unauthorized access to company systems and customer data.

For stronger protection, the organization should prioritize phishing-resistant multifactor methods, particularly FIDO2/WebAuthn security keys or platform authenticators, for accounts with access to sensitive systems. These methods provide strong resistance to credential phishing and replay attacks. The organization should also apply the control broadly, with particular attention to administrative, remote-access, cloud-service, and customer-data access paths, and should maintain secure account-recovery procedures so that recovery cannot bypass the added assurance. This is consistent with NIST guidance that multifactor authentication uses more than one distinct authentication factor and substantially improves assurance over password-only authentication. See NIST SP 800-63B: Authentication and Authenticator Management and CISA: Turn On Multifactor Authentication.

**QUESTION NO: 17**

Which action should an IT department take if an organization decides to expand its business by selling products online?

**A.** Make sure the website can handle e-commerce transactions

**B.** Ensure that the strategic goals aligned with the organization's mission statement

**C.** Market the companyâ€™s products or services

**D.** Manage capital to ensure a successful website

**ANSWER: A**

**Explanation:**

Making sure the website can handle e-commerce transactions is the appropriate IT action because moving sales online creates a technology capability that must be reliable, secure, and integrated with business operations. The IT department should ensure the site and supporting infrastructure can securely accept, authorize, and record payments; protect customer and cardholder data in transit and at rest; and maintain availability as transaction volume and customer traffic grow. This also includes integrating the e-commerce storefront with inventory, order-management, fulfillment, and customer-service systems so that product availability, orders, and customer records remain accurate. For payment-card transactions, the organization’s environment and service providers must meet applicable PCI DSS requirements. PCI SSC describes PCI DSS as a baseline of technical and operational requirements designed to protect payment account data, including requirements for secure systems, access control, monitoring, and testing. Secure development and deployment practices are likewise essential for preventing common web-application risks affecting online purchasing workflows. These operational, security, and integration responsibilities fall directly within IT’s role in enabling a dependable online sales channel. See the PCI Security Standards Council PCI DSS overview and the OWASP Top 10 Web Application Security Risks.

**QUESTION NO: 18**

An organization is moving a records-management application to an infrastructure as a service (IaaS) cloud environment. The security team must identify responsibilities that remain with the organization under the shared responsibility model.

Which two responsibilities remain with the organization? Choose 2 answers.

**A.** Patching and hardening guest operating systems

**B.** Providing physical security for cloud data centers

**C.** Configuring identity and access permissions for organizational data

**D.** Replacing failed physical host hardware

**E.** Operating the cloud provider's physical network backbone

**ANSWER: A C**

**Explanation:**

In an IaaS deployment, the organization remains responsible for securing the guest operating systems and the applications it installs and operates. This includes patching and hardening virtual machines, configuring host controls, and managing application security. The organization is also responsible for configuring access to its data, including identity permissions, network security groups, encryption choices, and data classification requirements.

The cloud provider is generally responsible for the physical security of the data centers and for operating the underlying physical infrastructure. Although customers must select and configure cloud services securely, they do not operate the provider's physical facilities or maintain the provider's physical hosts.

## QUESTION NO: 19

Which two languages are scripted?

Choose 2 answers

**A.** Python

**B.** Ada

**C.** PHP

**D.** C

**ANSWER: A C**

**Explanation:**

Python and PHP are correctly identified as scripting languages. Python is a high-level, interpreted language commonly used to automate tasks, create administrative tools, process data, develop web applications, and integrate systems through scripts. Its runtime execution model and broad standard library make it particularly useful for security automation and orchestration tasks. The Python Software Foundation describes Python as an interpreted, high-level language with an emphasis on readability and rapid development.

PHP is also a scripting language, most notably for server-side web development. A web server can execute PHP code to generate dynamic content, interact with databases, manage sessions, and implement application logic before returning a response to a client. PHP's official documentation specifically describes it as a popular general-purpose scripting language that is especially suited to web development and can be embedded in HTML. In cybersecurity architecture and engineering, recognizing these as scripted languages helps distinguish code commonly executed by an interpreter or runtime from traditionally compiled systems languages.

References: Python.org: What is Python? and PHP Manual: What is PHP?.

## QUESTION NO: 20

How does application software differ from operating systems?

Choose 2 answers

**A.** Application software includes system utilities that run on demand of the user.

**B.** Application software consists of programs that end users run to accomplish business or personal tasks, such as e-mail.

**C.** Application software includes word processors and spreadsheet software that are useful to end users.

**D.** Application software supports the computer hardware system directly.

## ANSWER: B C

**Explanation:**

Application software consists of programs that end users run to accomplish business or personal tasks, such as e-mail, because it is designed to help people directly perform a particular activity. An email client, for example, gives a user the functions needed to compose, send, receive, organize, and search messages. These user-focused capabilities distinguish application programs from the operating system, which provides the underlying execution environment and manages shared system resources.

Application software includes word processors and spreadsheet software that are useful to end users because these programs support concrete productivity tasks: creating and formatting documents, performing calculations, analyzing data, and presenting information. A word processor or spreadsheet runs on top of an operating system and uses operating-system services, such as file storage, memory allocation, display access, and networking, rather than managing those resources as its primary role. This layered relationship is a core computing concept: the operating system acts as the intermediary between applications, users, and hardware, while applications provide task-specific functionality. See the NIST Guide to Information Security Terms and Microsoft's overview of operating-system services.

## QUESTION NO: 21

A healthcare organization has experienced a ransomware attack that has resulted in the encryption of all patient medical records. The organization has backups, but restoring the data will take severaldays, and during that time, patient care will be significantly diminished.

What is the most important factor to consider when evaluating the severity of the ransomware attack?

**A.** Threat actors

**B.** Risk

**C.** Impact

**D.** Likelihood

## ANSWER: C

**Explanation:**

Impact is the most important factor because the incident has already disrupted the organization's ability to provide healthcare. Encryption of all patient medical records prevents timely access to information clinicians need for diagnosis, treatment, medication decisions, and continuity of care. Although backups permit eventual recovery, the several-day restoration period creates an immediate and substantial operational effect: patient care is significantly diminished. In a healthcare environment, this can also create patient-safety concerns and may require downtime procedures, diversion of services, or delays in treatment.

Incident severity is assessed primarily by the actual and potential consequences to the organization, its mission, and affected individuals. Here, the scope of unavailable records and the duration of the outage demonstrate a high-impact event. This assessment guides prioritization of incident-response resources, executive escalation, recovery sequencing,

communications, and any required regulatory or legal actions. The ransomware event is therefore severe because of its effect on essential clinical operations, not merely because data was encrypted or recovery is possible.

NIST's incident-handling guidance emphasizes analyzing incident impact to support response and prioritization decisions: NIST SP 800-61 Rev. 2. HHS also identifies ransomware as a major threat to healthcare operations and patient safety: HHS Ransomware Fact Sheet.

## QUESTION NO: 22

An employee needs to execute a program from the command line.

Which peripheral device should be used?

**A.** Keyboard

**B.** Hard drive

**C.** Speaker

**D.** Printer

## ANSWER: A

**Explanation:**

**Keyboard** is the appropriate peripheral because a command-line interface requires the user to enter textual commands and any required parameters. A keyboard is an input device designed to send keystrokes to the operating system or terminal application, allowing the employee to type a program name or path and execute it, commonly by pressing Enter. For example, a user may enter a command such as `python script.py`, `ipconfig`, or a shell script command in a terminal. The command interpreter receives this keyboard input, parses the command, and asks the operating system to start the requested process. Command-line environments also use the keyboard for navigation, editing commands, supplying interactive responses, and interrupting a running process when necessary. This makes the keyboard the essential human-interface peripheral for direct command-line operation. Microsoft's overview of command-line tools describes using Command Prompt to run commands and programs: Windows Commands documentation. The Linux command-line documentation likewise describes entering commands at a shell prompt: GNU Bash Reference Manual.

## QUESTION NO: 23

Which two options allow an application to access a database?

Choose 2 answers

**A.** Structured Query Language (SQL)

**B.** Java Database Connectivity (JDBC)

**C.** Database management system (DBMS)

**D.** Open Database Connectivity (ODBC)

**E.** Graphical user interface (GUI)

## ANSWER: B D

**Explanation:**

Java Database Connectivity (JDBC) and Open Database Connectivity (ODBC) are database connectivity interfaces that enable an application to establish a connection to a database, send requests, and receive results. JDBC is Java's standard API for database access. A Java application commonly uses a JDBC driver and connection string to connect to a database management system, then executes SQL statements through JDBC objects such as connections, statements, and result

sets. Oracle’s JDBC overview describes JDBC as the Java API for accessing relational data, including connecting to databases and executing SQL: Oracle JDBC documentation.

Open Database Connectivity (ODBC) is a language-independent, standardized interface for database access. An application uses an ODBC driver to communicate with a particular database platform through the ODBC API, allowing software written in many languages to access data without being tied to a database-specific interface. Microsoft documents ODBC as an interface that applications use to access data in database management systems through drivers: Microsoft ODBC overview. Both JDBC and ODBC therefore provide the application-facing connectivity layer needed to access a database.