

## CISSP Dumps

# Certified Information Systems Security Professional (CISSP)

<https://www.certleader.com/CISSP-dumps.html>



#### NEW QUESTION 1

- (Exam Topic 15)

In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

- A. Organizational Security Policy
- B. Security Target (ST)
- C. Protection Profile (PP)
- D. Target of Evaluation (TOE)

**Answer:** C

#### NEW QUESTION 2

- (Exam Topic 15)

Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using which protocol?

- A. Secure Shell (SSH)
- B. Internet Protocol Security (IPsec)
- C. Secure Sockets Layer (SSL)
- D. Extensible Authentication Protocol (EAP)

**Answer:** A

#### NEW QUESTION 3

- (Exam Topic 15)

Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

- A. Proper security controls, security goals, and fault mitigation are properly conducted.
- B. Proper security controls, security objectives, and security goals are properly initiated.
- C. Security goals, proper security controls, and validation are properly initiated.
- D. Security objectives, security goals, and system test are properly conducted.

**Answer:** B

#### NEW QUESTION 4

- (Exam Topic 15)

While reviewing the financial reporting risks of a third-party application, which of the following Service Organization Control (SOC) reports will be the MOST useful?

- A. ISIsOC 1
- B. SOC 2
- C. SOC 3
- D. SOC for cybersecurity

**Answer:** A

#### NEW QUESTION 5

- (Exam Topic 15)

Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-systems gracefully handle invalid input?

- A. Unit testing
- B. Integration testing
- C. Negative testing
- D. Acceptance testing

**Answer:** B

#### NEW QUESTION 6

- (Exam Topic 15)

Which of the following access control models is MOST restrictive?

- A. Discretionary Access Control (DAC)
- B. Mandatory Access Control (MAC)
- C. Role Based Access Control (RBAC)
- D. Rule based access control

**Answer:** B

#### NEW QUESTION 7

- (Exam Topic 15)

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes.

What is the

BEST design approach to securing this environment?

- A. Place firewalls around critical devices, isolating them from the rest of the environment.
- B. Layer multiple detective and preventative technologies at the environment perimeter.

- C. Use reverse proxies to create a secondary "shadow" environment for critical systems.
- D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

**Answer:** B

#### NEW QUESTION 8

- (Exam Topic 15)

Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-system gracefully handle invalid input?

- A. Negative testing
- B. Integration testing
- C. Unit testing
- D. Acceptance testing

**Answer:** B

#### NEW QUESTION 9

- (Exam Topic 15)

What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

- A. ICS often do not have availability requirements.
- B. ICS are often isolated and difficult to access.
- C. ICS often run on UNIX operating systems.
- D. ICS are often sensitive to unexpected traffic.

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 15)

Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

- A. Application threat modeling
- B. Secure software development.
- C. Agile software development
- D. Penetration testing

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 15)

Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

- A. Employee evaluation of the training program
- B. Internal assessment of the training program's effectiveness
- C. Multiple choice tests to participants
- D. Management control of reviews

**Answer:** B

#### NEW QUESTION 15

- (Exam Topic 15)

Recently, an unknown event has disrupted a single Layer-2 network that spans between two geographically diverse data centers. The network engineers have asked for assistance in identifying the root cause of the event. Which of the following is the MOST likely cause?

- A. Misconfigured routing protocol
- B. Smurf attack
- C. Broadcast domain too large
- D. Address spoofing

**Answer:** D

#### NEW QUESTION 19

- (Exam Topic 15)

What is the PRIMARY benefit of incident reporting and computer crime investigations?

- A. Providing evidence to law enforcement
- B. Repairing the damage and preventing future occurrences
- C. Appointing a computer emergency response team
- D. Complying with security policy

**Answer:** D

#### NEW QUESTION 23

- (Exam Topic 15)

What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

- A. Man-in-the-Middle (MITM)
- B. Denial of Service (DoS)
- C. Domain Name Server (DNS) poisoning
- D. Buffer overflow

**Answer:** B

**NEW QUESTION 25**

- (Exam Topic 15)

A user is allowed to access the file labeled “Financial Forecast,” but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

- A. Minimum access control
- B. Rule-based access control
- C. Limited role-based access control (RBAC)
- D. Access control list (ACL)

**Answer:** B

**NEW QUESTION 29**

- (Exam Topic 15)

Which of the following types of firewall only examines the “handshaking” between packets before forwarding traffic?

- A. Proxy firewalls
- B. Host-based firewalls
- C. Circuit-level firewalls
- D. Network Address Translation (NAT) firewalls

**Answer:** C

**NEW QUESTION 33**

- (Exam Topic 15)

What method could be used to prevent passive attacks against secure voice communications between an organization and its vendor?

- A. Encryption in transit
- B. Configure a virtual private network (VPN)
- C. Configure a dedicated connection
- D. Encryption at rest

**Answer:** A

**NEW QUESTION 37**

- (Exam Topic 15)

Which of the following regulations dictates how data breaches are handled?

- A. Sarbanes-Oxley (SOX)
- B. National Institute of Standards and Technology (NIST)
- C. Payment Card Industry Data Security Standard (PCI-DSS)
- D. General Data Protection Regulation (GDPR)

**Answer:** D

**NEW QUESTION 42**

- (Exam Topic 15)

A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

- A. Availability
- B. Disaster recovery (DR)
- C. Redundancy
- D. Business continuity (BC)

**Answer:** D

**NEW QUESTION 46**

- (Exam Topic 15)

Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users internal control over financial reporting?

- A. Statement on Auditing Standards (SAS)70
- B. Service Organization Control 1 (SOC1)
- C. Service Organization Control 2 (SOC2)
- D. Service Organization Control 3 (SOC3)

**Answer:** B

**NEW QUESTION 50**

- (Exam Topic 15)

Which of the following phases in the software acquisition process does developing evaluation criteria take place?

- A. Follow-On
- B. Planning
- C. Contracting
- D. Monitoring and Acceptance

**Answer:** D

**NEW QUESTION 54**

- (Exam Topic 15)

What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

- A. Configuration management (CM)
- B. Information Rights Management (IRM)
- C. Policy creation
- D. Data classification

**Answer:** D

**NEW QUESTION 59**

- (Exam Topic 15)

What is the correct order of execution for security architecture?

- A. Governance, strategy and program management, project delivery, operations
- B. Strategy and program management, governance, project delivery, operations
- C. Governance, strategy and program management, operations, project delivery
- D. Strategy and program management, project delivery, governance, operations

**Answer:** A

**NEW QUESTION 64**

- (Exam Topic 15)

Which of the following is the MOST common cause of system or security failures?

- A. Lack of system documentation
- B. Lack of physical security controls
- C. Lack of change control
- D. Lack of logging and monitoring

**Answer:** D

**NEW QUESTION 69**

- (Exam Topic 15)

What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

- A. Capturing an image of the system
- B. Maintaining the chain of custody
- C. Complying with the organization's security policy
- D. Outlining all actions taken during the investigation

**Answer:** A

**NEW QUESTION 72**

- (Exam Topic 15)

In which of the following system life cycle processes should security requirements be developed?

- A. Risk management
- B. Business analysis
- C. Information management
- D. System analysis

**Answer:** B

**NEW QUESTION 76**

- (Exam Topic 15)

Which of the following is the MOST effective countermeasure against data remanence?

- A. Destruction
- B. Clearing
- C. Purging
- D. Encryption

**Answer:** A

**NEW QUESTION 77**

- (Exam Topic 15)

Which of the following BEST represents a defense in depth concept?

- A. Network-based data loss prevention (DLP), Network Access Control (NAC), network-based Intrusion prevention system (NIPS), Port security on core switches
- B. Host-based data loss prevention (DLP), Endpoint anti-malware solution, Host-based integrity checker, Laptop locks, hard disk drive (HDD) encryption
- C. Endpoint security management, network intrusion detection system (NIDS), Network Access Control (NAC), Privileged Access Management (PAM), security information and event management (SIEM)
- D. Web application firewall (WAF), Gateway network device tuning, Database firewall, Next-Generation Firewall (NGFW), Tier-2 demilitarized zone (DMZ) tuning

**Answer:** C

**NEW QUESTION 78**

- (Exam Topic 15)

Which of the following criteria ensures information is protected relative to its importance to the organization?

- A. The value of the data to the organization's senior management
- B. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification
- C. Legal requirements determined by the organization headquarters' location
- D. Organizational stakeholders, with classification approved by the management board

**Answer:** D

**NEW QUESTION 79**

- (Exam Topic 15)

Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

- A. For the establishment, exercise, or defense of legal claims
- B. The personal data has been lawfully processed and collected
- C. The personal data remains necessary to the purpose for which it was collected
- D. For the reasons of private interest

**Answer:** C

**NEW QUESTION 81**

- (Exam Topic 15)

Which of the following is a Key Performance Indicator (KPI) for a security training and awareness program?

- A. The number of security audits performed
- B. The number of attendees at security training events
- C. The number of security training materials created
- D. The number of security controls implemented

**Answer:** B

**NEW QUESTION 83**

- (Exam Topic 15)

In software development, which of the following entities normally signs the code to protect the code integrity?

- A. The organization developing the code
- B. The quality control group
- C. The data owner
- D. The developer

**Answer:** B

**NEW QUESTION 84**

- (Exam Topic 15)

A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

- A. Email the policy to the colleague as they were already part of the organization and familiar with it.
- B. Do not acknowledge receiving the request from the former colleague and ignore them.
- C. Access the policy on a company-issued device and let the former colleague view the screen.
- D. Submit the request using company official channels to ensure the policy is okay to distribute.

**Answer:** B

**NEW QUESTION 89**

- (Exam Topic 15)

Before implementing an internet-facing router, a network administrator ensures that the equipment is baselined/hardened according to approved configurations and settings. This action provides protection against which of the following attacks?

- A. Blind spoofing
- B. Media Access Control (MAC) flooding
- C. SQL injection (SQLI)



D. Ransomware

**Answer: B**

**NEW QUESTION 93**

- (Exam Topic 15)

Which of the following terms BEST describes a system which allows a user to log in and access multiple related servers and applications?

- A. Remote Desktop Protocol (RDP)
- B. Federated identity management (FIM)
- C. Single sign-on (SSO)
- D. Multi-factor authentication (MFA)

**Answer: B**

**NEW QUESTION 96**

- (Exam Topic 15)

An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

- A. IM clients can interoperate between multiple vendors.
- B. IM clients can run without administrator privileges.
- C. IM clients can utilize random port numbers.
- D. IM clients can run as executable that do not require installation.

**Answer: B**

**NEW QUESTION 101**

- (Exam Topic 15)

While classifying credit card data related to Payment Card Industry Data Security Standards (PCI-DSS), which of the following is a PRIMARY security requirement?

- A. Processor agreements with card holders
- B. Three-year retention of data
- C. Encryption of data
- D. Specific card disposal methodology

**Answer: C**

**NEW QUESTION 103**

- (Exam Topic 15)

What BEST describes the confidentiality, integrity, availability triad?

- A. A tool used to assist in understanding how to protect the organization's data
- B. The three-step approach to determine the risk level of an organization
- C. The implementation of security systems to protect the organization's data
- D. A vulnerability assessment to see how well the organization's data is protected

**Answer: C**

**NEW QUESTION 105**

- (Exam Topic 15)

Security Software Development Life Cycle (SDLC) expects application code to be written in a consistent manner to allow ease of auditing and which of the following?

- A. Protecting
- B. Executing
- C. Copying
- D. Enhancing

**Answer: A**

**NEW QUESTION 108**

- (Exam Topic 15)

Which of the following is the PRIMARY purpose of due diligence when an organization embarks on a merger or acquisition?

- A. Assess the business risks.
- B. Formulate alternative strategies.
- C. Determine that all parties are equally protected.
- D. Provide adequate capability for all parties.
- E. Strategy and program management, project delivery, governance, operations

**Answer: A**

**NEW QUESTION 109**

- (Exam Topic 15)

What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

- A. Save security costs for the organization.
- B. Improve vulnerability assessment capabilities.
- C. Standardize specifications between software security products.
- D. Achieve organizational compliance with international standards.

**Answer: C**

**NEW QUESTION 113**

- (Exam Topic 15)

Which of the following is the BEST way to protect privileged accounts?

- A. Quarterly user access rights audits
- B. Role-based access control (RBAC)
- C. Written supervisory approval
- D. Multi-factor authentication (MFA)

**Answer: D**

**NEW QUESTION 115**

- (Exam Topic 15)

The acquisition of personal data being obtained by a lawful and fair means is an example of what principle?

- A. Data Quality Principle
- B. Openness Principle
- C. Purpose Specification Principle
- D. Collection Limitation Principle

**Answer: D**

**NEW QUESTION 116**

- (Exam Topic 15)

A Distributed Denial of Service (DDoS) attack was carried out using malware called Mirai to create a large-scale command and control system to launch a botnet.

Which of the following devices were the PRIMARY sources used to generate the attack traffic?

- A. Internet of Things (IoT) devices
- B. Microsoft Windows hosts
- C. Web servers running open source operating systems (OS)
- D. Mobile devices running Android

**Answer: A**

**NEW QUESTION 118**

- (Exam Topic 15)

Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

- A. Sniffing the traffic of a compromised host inside the network
- B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network
- C. A brute force password attack on the Secure Shell (SSH) port of the controller
- D. Remote Authentication Dial-In User Service (RADIUS) token replay attack

**Answer: B**

**NEW QUESTION 119**

- (Exam Topic 15)

When conducting a third-party risk assessment of a new supplier, which of the following reports should be reviewed to confirm the operating effectiveness of the security, availability, confidentiality, and privacy trust principles?

- A. Service Organization Control (SOC) 1, Type 2
- B. Service Organization Control (SOC) 2, Type 2
- C. International Organization for Standardization (ISO) 27001
- D. International Organization for Standardization (ISO) 27002

**Answer: B**

**NEW QUESTION 121**

- (Exam Topic 15)

Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

- A. Training department
- B. Internal audit
- C. Human resources
- D. Information technology (IT)

**Answer: C**



**NEW QUESTION 123**

- (Exam Topic 15)

Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

- A. RJ11
- B. LC ports
- C. Patch panel
- D. F-type connector

**Answer:** C

**NEW QUESTION 125**

- (Exam Topic 15)

A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

- A. Pinning
- B. Single-pass wipe
- C. Degaussing
- D. Multi-pass wipes

**Answer:** C

**NEW QUESTION 127**

- (Exam Topic 15)

If an employee transfers from one role to another, which of the following actions should this trigger within the identity and access management (IAM) lifecycle?

- A. New account creation
- B. User access review and adjustment
- C. Deprovisioning
- D. System account access review and adjustment

**Answer:** B

**NEW QUESTION 131**

- (Exam Topic 15)

Which of the following BEST obtains an objective audit of security controls?

- A. The security audit is measured against a known standard.
- B. The security audit is performed by a certified internal auditor.
- C. The security audit is performed by an independent third-party.
- D. The security audit produces reporting metrics for senior leadership.

**Answer:** A

**NEW QUESTION 132**

- (Exam Topic 15)

Which of the following is a unique feature of attribute-based access control (ABAC)?

- A. A user is granted access to a system based on group affinity.
- B. A user is granted access to a system with biometric authentication.
- C. A user is granted access to a system at a particular time of day.
- D. A user is granted access to a system based on username and password.

**Answer:** C

**NEW QUESTION 133**

- (Exam Topic 15)

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

- A. Change driver
- B. Change implementer
- C. Program sponsor
- D. Project manager

**Answer:** D

**NEW QUESTION 135**

- (Exam Topic 15)

What is the FIRST step in risk management?

- A. Establish the expectations of stakeholder involvement.
- B. Identify the factors that have potential to impact business.
- C. Establish the scope and actions required.
- D. Identify existing controls in the environment.

**Answer: C**

**NEW QUESTION 140**

- (Exam Topic 15)

Which of the following BEST describes why software assurance is critical in helping prevent an increase in business and mission risk for an organization?

- A. Software that does not perform as intended may be exploitable which makes it vulnerable to attack.
- B. Request for proposals (RFP) avoid purchasing software that does not meet business needs.
- C. Contracting processes eliminate liability for security vulnerabilities for the purchaser.
- D. Decommissioning of old software reduces long-term costs related to technical debt.

**Answer: B**

**NEW QUESTION 142**

- (Exam Topic 15)

Which of the following is TRUE for an organization that is using a third-party federated identity service?

- A. The organization enforces the rules to other organization's user provisioning
- B. The organization establishes a trust relationship with the other organizations
- C. The organization defines internal standard for overall user identification
- D. The organization specifies alone how to authenticate other organization's users

**Answer: C**

**NEW QUESTION 145**

- (Exam Topic 15)

A new site's gateway isn't able to form a tunnel to the existing site-to-site Internet Protocol Security (IPsec) virtual private network (VPN) device at headquarters. Devices at the new site have no problem accessing resources on the Internet. When testing connectivity between the remote site's gateway, it was observed that the external Internet Protocol (IP) address of the gateway was set to 192.168.1.1. and was configured to send outbound traffic to the Internet Service Provider (ISP) gateway at 192.168.1.2. Which of the following would be the BEST way to resolve the issue and get the remote site connected?

- A. Enable IPsec tunnel mode on the VPN devices at the new site and the corporate headquarters.
- B. Enable Layer 2 Tunneling Protocol (L2TP) on the VPN devices at the new site and the corporate headquarters.
- C. Enable Point-to-Point Tunneling Protocol (PPTP) on the VPN devices at the new site and the corporate headquarters.
- D. Enable Network Address Translation (NAT) - Traversal on the VPN devices at the new site and the corporate headquarters.

**Answer: A**

**NEW QUESTION 149**

- (Exam Topic 15)

Which of the following is the MOST appropriate technique for destroying magnetic platter style hard disk drives (HDD) containing data with a "HIGH" security categorization?

- A. Drill through the device and platters.
- B. Mechanically shred the entire HDD.
- C. Remove the control electronics.
- D. HP iProcess the HDD through a degaussing device.

**Answer: D**

**NEW QUESTION 152**

- (Exam Topic 15)

Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

- A. Store sensitive data only when necessary.
- B. Educate end-users on methods of attacks on sensitive data.
- C. Establish report parameters for sensitive data.
- D. Monitor mail servers for sensitive data being exfiltrated.

**Answer: A**

**NEW QUESTION 153**

- (Exam Topic 15)

An organization is implementing data encryption using symmetric ciphers and the Chief Information Officer (CIO) is concerned about the risk of using one key to protect all sensitive data, The security practitioner has been tasked with recommending a solution to address the CIO's concerns, Which of the following is the BEST approach to achieving the objective by encrypting all sensitive data?

- A. Use a Secure Hash Algorithm 256 (SHA-256).
- B. Use a hierarchy of encryption keys.
- C. Use Hash Message Authentication Code (HMAC) keys.
- D. Use Rivest-Shamir-Adleman (RSA) keys.

**Answer: D**

**NEW QUESTION 158**

- (Exam Topic 15)

A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

- A. Statically typed
- B. Weakly typed
- C. Strongly typed
- D. Dynamically typed

**Answer:** D

#### NEW QUESTION 161

- (Exam Topic 15)

A recent security audit is reporting several unsuccessful login attempts being repeated at specific times during the day on an Internet facing authentication server. No alerts have been generated by the security information and event management (SIEM) system. What PRIMARY action should be taken to improve SIEM performance?

- A. Implement role-based system monitoring
- B. Audit firewall logs to identify the source of login attempts
- C. Enhance logging detail
- D. Confirm alarm thresholds

**Answer:** B

#### NEW QUESTION 162

- (Exam Topic 15)

In Identity Management (IdM), when is the verification stage performed?

- A. As part of system sign-on
- B. Before creation of the identity
- C. After revocation of the identity
- D. During authorization of the identity

**Answer:** A

#### NEW QUESTION 167

- (Exam Topic 15)

Digital non-repudiation requires which of the following?

- A. A trusted third-party
- B. Appropriate corporate policies
- C. Symmetric encryption
- D. Multifunction access cards

**Answer:** A

#### NEW QUESTION 172

- (Exam Topic 15)

Which of the following is the MOST important first step in preparing for a security audit?

- A. Identify team members.
- B. Define the scope.
- C. Notify system administrators.
- D. Collect evidence.

**Answer:** B

#### NEW QUESTION 173

- (Exam Topic 15)

Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

- A. Control traffic
- B. Prevent rapid movement
- C. Prevent piggybacking
- D. Control air flow

**Answer:** C

#### NEW QUESTION 176

- (Exam Topic 15)

Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

- A. Take photos of the damage
- B. Notify all of the Board of Directors
- C. Communicate with the press following the communications plan
- D. Dispatch personnel to the disaster recovery (DR) site

**Answer:** A

**NEW QUESTION 178**

- (Exam Topic 15)

A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS).

Which of the following factors leads the company to choose an IDaaS as their solution?

- A. In-house development provides more control.
- B. In-house team lacks resources to support an on-premise solution.
- C. Third-party solutions are inherently more secure.
- D. Third-party solutions are known for transferring the risk to the vendor.

**Answer:** B

**NEW QUESTION 181**

- (Exam Topic 15)

Which technique helps system designers consider potential security concerns of their systems and applications?

- A. Penetration testing
- B. Threat modeling
- C. Manual inspections and reviews
- D. Source code review

**Answer:** B

**NEW QUESTION 184**

- (Exam Topic 15)

When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

- A. The actual origin and tools used for the test can be hidden.
- B. Information may be found on related breaches and hacking.
- C. Vulnerabilities can be tested without impact on the tested environment.
- D. Information may be found on hidden vendor patches.

**Answer:** D

**NEW QUESTION 186**

- (Exam Topic 15)

A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

- A. Federation authorities
- B. Proxied federation
- C. Static registration
- D. Dynamic registration

**Answer:** D

**NEW QUESTION 187**

- (Exam Topic 15)

Before allowing a web application into the production environment, the security practitioner performs multiple types of tests to confirm that the web application performs as expected. To test the username field, the security practitioner creates a test that enters more characters into the field than is allowed. Which of the following BEST describes the type of test performed?

- A. Misuse case testing
- B. Penetration testing
- C. Web session testing
- D. Interface testing

**Answer:** A

**NEW QUESTION 188**

- (Exam Topic 15)

Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

- A. Integrity
- B. Scalability
- C. Availability
- D. Confidentiality

**Answer:** A

**NEW QUESTION 193**

- (Exam Topic 15)

When telephones in a city are connected by a single exchange, the caller can only connect with the switchboard operator. The operator then manually connects the call.

This is an example of which type of network topology?

- A. Star
- B. Tree
- C. Point-to-Point Protocol (PPP)
- D. Bus

**Answer:** A

#### NEW QUESTION 197

- (Exam Topic 15)

Secure coding can be developed by applying which one of the following?

- A. Applying the organization's acceptable use guidance
- B. Applying the industry best practice coding guidelines
- C. Applying rapid application development (RAD) coding
- D. Applying the organization's web application firewall (WAF) policy

**Answer:** B

#### NEW QUESTION 201

- (Exam Topic 15)

A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

- A. Intrusion prevention system (IPS)
- B. Multi-factor authentication (MFA)
- C. Data loss protection (DLP)
- D. Data at rest encryption

**Answer:** B

#### NEW QUESTION 203

- (Exam Topic 15)

A company wants to store data related to users on an offsite server. What method can be deployed to protect the privacy of the user's information while maintaining the field-level configuration of the database?

- A. Encryption
- B. Encoding
- C. Tokenization
- D. Hashing

**Answer:** A

#### NEW QUESTION 205

- (Exam Topic 15)

In software development, developers should use which type of queries to prevent a Structured Query Language (SQL) injection?

- A. Parameterised
- B. Dynamic
- C. Static
- D. Controlled

**Answer:** A

#### NEW QUESTION 208

- (Exam Topic 15)

While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

- A. Detective and recovery controls
- B. Corrective and recovery controls
- C. Preventative and corrective controls
- D. Recovery and proactive controls

**Answer:** C

#### NEW QUESTION 210

- (Exam Topic 15)

In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

- A. Development/Acquisition
- B. Initiation
- C. Implementation/ Assessment
- D. Disposal

**Answer:** A

**NEW QUESTION 215**

- (Exam Topic 15)

A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

- A. Upgrade the software affected by the vulnerability.
- B. Inform management of possible risks.
- C. Mitigate the risks with compensating controls.
- D. Remove the affected software from the servers.

**Answer:** C

**NEW QUESTION 217**

- (Exam Topic 15)

When conducting a remote access session using Internet Protocol Security (IPSec), which Open Systems Interconnection (OSI) model layer does this connection use?

- A. Transport
- B. Network
- C. Data link
- D. Presentation

**Answer:** B

**NEW QUESTION 219**

- (Exam Topic 15)

Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

- A. Prevent information about browsing activities from being stored in the cloud.
- B. Store browsing activities in the cloud.
- C. Prevent information about browsing activities from being stored on the personal device.
- D. Store information about browsing activities on the personal device.

**Answer:** A

**NEW QUESTION 223**

- (Exam Topic 15)

Which type of access control includes a system that allows only users that are type=managers and department=sales to access employee records?

- A. Discretionary access control (DAC)
- B. Mandatory access control (MAC)
- C. Role-based access control (RBAC)
- D. Attribute-based access control (ABAC)

**Answer:** C

**NEW QUESTION 224**

- (Exam Topic 15)

Which of the following is the FIRST step during digital identity provisioning?

- A. Authorizing the entity for resource access
- B. Synchronizing directories
- C. Issuing an initial random password
- D. Creating the entity record with the correct attributes

**Answer:** D

**NEW QUESTION 225**

- (Exam Topic 15)

Which of the following is the name of an individual or group that is impacted by a change?

- A. Change agent
- B. Stakeholder
- C. Sponsor
- D. End User

**Answer:** B

**NEW QUESTION 229**

- (Exam Topic 15)

What is the MAIN purpose of a security assessment plan?

- A. Provide guidance on security requirements, to ensure the identified security risks are properly addressed based on the recommendation



- B. Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.
- C. Provide technical information to executives to help them understand information security postures and secure funding.
- D. Provide education to employees on security and privacy, to ensure their awareness on policies and procedures

**Answer:** B

#### NEW QUESTION 231

- (Exam Topic 15)

Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

- A. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools
- B. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools
- C. Maintaining the inventory through a combination of on-premise storage configuration, cloud management, and partner management tools
- D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

**Answer:** C

#### NEW QUESTION 233

- (Exam Topic 15)

A security professional can BEST mitigate the risk of using a Commercial Off-The-Shelf (COTS) solution by deploying the application with which of the following controls in ?

- A. Whitelisting application
- B. Network segmentation
- C. Hardened configuration
- D. Blacklisting application

**Answer:** A

#### NEW QUESTION 237

- (Exam Topic 15)

What is the FIRST step prior to executing a test of an organisation's disaster recovery (DR) or business continuity plan (BCP)?

- A. identify key stakeholders,
- B. Develop recommendations for disaster scenarios.
- C. Identify potential failure points.
- D. Develop clear evaluation criteria.

**Answer:** D

#### NEW QUESTION 242

- (Exam Topic 15)

The application owner of a system that handles confidential data leaves an organization. It is anticipated that a replacement will be hired in approximately six months. During that time, which of the following should the organization do?

- A. Grant temporary access to the former application owner's account
- B. Assign a temporary application owner to the system.
- C. Restrict access to the system until a replacement application owner is hired.
- D. Prevent changes to the confidential data until a replacement application owner is hired.

**Answer:** B

#### NEW QUESTION 244

- (Exam Topic 15)

The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a particular system over a 12-month period. Which type of SOC report should be utilized?

- A. SOC 1 Type 1
- B. SOC 2 Type 2
- C. SOC 2 Type 2
- D. SOC 3 Type 1

**Answer:** C

#### NEW QUESTION 246

- (Exam Topic 15)

A company needs to provide employee access to travel services, which are hosted by a third-party service provider. Employee experience is important, and when users are already authenticated, access to the travel portal is seamless. Which of the following methods is used to share information and grant user access to the travel portal?

- A. Security Assertion Markup Language (SAML) access
- B. Single sign-on (SSO) access
- C. Open Authorization (OAuth) access
- D. Federated access

**Answer:** D

**NEW QUESTION 249**

- (Exam Topic 15)

employee training, risk management, and data handling procedures and policies could be characterized as which type of security measure?

- A. Non-essential
- B. Management
- C. Preventative
- D. Administrative

**Answer:** D

**NEW QUESTION 252**

- (Exam Topic 15)

An information security professional is reviewing user access controls on a customer-facing application. The application must have multi-factor authentication (MFA) in place. The application currently requires a username and password to login. Which of the following options would BEST implement MFA?

- A. Geolocate the user and compare to previous logins
- B. Require a pre-selected number as part of the login
- C. Have the user answer a secret question that is known to them
- D. Enter an automatically generated number from a hardware token

**Answer:** C

**NEW QUESTION 257**

- (Exam Topic 15)

Which of the following roles is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications?

- A. Data Reviewer
- B. Data User
- C. Data Custodian
- D. Data Owner

**Answer:** D

**NEW QUESTION 259**

- (Exam Topic 15)

What is the HIGHEST priority in agile development?

- A. Selecting appropriate coding language
- B. Managing costs of product delivery
- C. Early and continuous delivery of software
- D. Maximizing the amount of code delivered

**Answer:** C

**NEW QUESTION 262**

- (Exam Topic 15)

The security architect has been mandated to assess the security of various brands of mobile devices. At what phase of the product lifecycle would this be MOST likely to occur?

- A. Disposal
- B. Implementation
- C. Development
- D. Operations and maintenance

**Answer:** C

**NEW QUESTION 264**

- (Exam Topic 15)

Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?

- A. System logs
- B. Anti-spyware
- C. Integrity checker
- D. Firewall logs

**Answer:** C

**NEW QUESTION 269**

- (Exam Topic 15)

In order to provide dual assurance in a digital signature system, the design MUST include which of the following?

- A. The public key must be unique for the signed document.
- B. signature process must generate adequate authentication credentials.
- C. The hash of the signed document must be present.
- D. The encrypted private key must be provided in the signing certificate.

**Answer:** B

**NEW QUESTION 272**

- (Exam Topic 15)

What type of risk is related to the sequences of value-adding and managerial activities undertaken in an organization?

- A. Demand risk
- B. Process risk
- C. Control risk
- D. Supply risk

**Answer:** B

**NEW QUESTION 277**

- (Exam Topic 15)

In an environment where there is not full administrative control over all network connected endpoints, such as a university where non-corporate devices are used, what is the BEST way to restrict access to the network?

- A. Use switch port security to limit devices connected to a particular switch port.
- B. Use of virtual local area networks (VLAN) to segregate users.
- C. Use a client-based Network Access Control (NAC) solution.
- D. Use a clientless Network Access Control (NAC) solution

**Answer:** A

**NEW QUESTION 279**

- (Exam Topic 15)

When are security requirements the LEAST expensive to implement?

- A. When identified by external consultants
- B. During the application rollout phase
- C. During each phase of the project cycle
- D. When built into application design

**Answer:** D

**NEW QUESTION 281**

- (Exam Topic 15)

Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

- A. Diffie-hellman (DH) key exchange: DH ( $\geq 2048$  bits) Symmetric Key: Advanced Encryption Standard (AES)  $> 128$  bits Digital Signature: Rivest-Shamir-Adleman (RSA) (1024 bits)
- B. Diffie-hellman (DH) key exchange: DH ( $\geq 2048$  bits) Symmetric Key: Advanced Encryption Standard (AES)  $> 128$  bits Digital Signature: Digital Signature Algorithm (DSA) ( $\geq 2048$  bits)
- C. Diffie-hellman (DH) key exchange: DH ( $\leq 1024$  bits) Symmetric Key: Blowfish Digital Signature: Rivest-Shamir-Adleman (RSA) ( $\geq 2048$  bits)
- D. Diffie-hellman (DH) key exchange: DH ( $\geq 2048$  bits) Symmetric Key: Advanced Encryption Standard (AES)  $< 128$  bits Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) ( $\geq 256$  bits)

**Answer:** C

**NEW QUESTION 284**

- (Exam Topic 15)

An organization contracts with a consultant to perform a System Organization Control (SOC) 2 audit on their internal security controls. An auditor documents a finding related to an Application Programming Interface (API) performing an action that is not aligned with the scope or objective of the system. Which trust service principle would be MOST applicable in this situation?

- A. Processing Integrity
- B. Availability
- C. Confidentiality
- D. Security

**Answer:** B

**NEW QUESTION 287**

- (Exam Topic 15)

While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team?

- A. Customer identifiers should be a variant of the user's government-issued ID number.
- B. Customer identifiers that do not resemble the user's government-issued ID number should be used.
- C. Customer identifiers should be a cryptographic hash of the user's government-issued ID number.
- D. Customer identifiers should be a variant of the user's name, for example, "jdoe" or "john.doe."

**Answer:** C

**NEW QUESTION 289**

- (Exam Topic 15)

The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

- A. Data masking and encryption of personal data
- B. Only to use encryption protocols approved by EU
- C. Anonymization of personal data when transmitted to sources outside the EU
- D. Never to store personal data of EU citizens outside the EU

**Answer: D**

**NEW QUESTION 290**

- (Exam Topic 15)

The initial security categorization should be done early in the system life cycle and should be reviewed periodically. Why is it important for this to be done correctly?

- A. It determines the security requirements.
- B. It affects other steps in the certification and accreditation process.
- C. It determines the functional and operational requirements.
- D. The system engineering process works with selected security controls.

**Answer: B**

**NEW QUESTION 295**

- (Exam Topic 15)

What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

- A. Randomizing data
- B. Swapping data
- C. Encrypting data
- D. Encoding data

**Answer: C**

**NEW QUESTION 296**

- (Exam Topic 15)

A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

- A. Update the service level agreement (SLA) to provide the organization the right to audit the vendor.
- B. Update the service level agreement (SLA) to require the vendor to provide security capabilities.
- C. Update the contract so that the vendor is obligated to provide security capabilities.
- D. Update the contract to require the vendor to perform security code reviews.

**Answer: C**

**NEW QUESTION 297**

- (Exam Topic 15)

A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should be an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

- A. SOC 1
- B. SOC 2 Type I
- C. SOC 2 Type II
- D. SOC 3

**Answer: D**

**NEW QUESTION 300**

- (Exam Topic 15)

Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

- A. Statement on Auditing Standards (SAS) 70
- B. Service Organization Control (SOC) 2
- C. Service Organization Control (SOC) 1
- D. Statement on Standards for Attestation Engagements (SSAE) 18

**Answer: B**

**NEW QUESTION 302**

- (Exam Topic 15)

The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

- A. biometric data cannot be changed.
- B. Separate biometric data streams require increased security.
- C. The biometric devices are unknown.
- D. Biometric data must be protected from disclosure.

**Answer:** A

**NEW QUESTION 304**

- (Exam Topic 15)

Which of the following system components enforces access controls on an object?

- A. Security perimeter
- B. Access control matrix
- C. Trusted domain
- D. Reference monitor

**Answer:** B

**NEW QUESTION 307**

- (Exam Topic 15)

Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

- A. Scheduled team review of coding style and techniques for vulnerability patterns
- B. Using automated programs to test for the latest known vulnerability patterns
- C. The regular use of production code routines from similar applications already in use
- D. Ensure code editing tools are updated against known vulnerability patterns

**Answer:** B

**NEW QUESTION 309**

- (Exam Topic 14)

What is a warm site when conducting Business continuity planning (BCP)

- A. A location, other than the normal facility, used to process data on a daily basis
- B. An area partially equipped with equipment and resources to recover business functions
- C. A place void of any resources or equipment except air conditioning and raised flooring
- D. An alternate facility that allows for Immediate cutover to enable continuation of business functions

**Answer:** B

**NEW QUESTION 311**

- (Exam Topic 14)

Activity to baseline, tailor, and scope security controls takes place during which National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) step?

- A. Authorize IS.
- B. Assess security controls.
- C. Categorize Information system (IS).
- D. Select security controls.

**Answer:** D

**NEW QUESTION 315**

- (Exam Topic 14)

Continuity of operations is BEST supported by which of the following?

- A. Confidentiality, availability, and reliability
- B. Connectivity, reliability, and redundancy
- C. Connectivity, reliability, and recovery
- D. Confidentiality, integrity, and availability

**Answer:** B

**NEW QUESTION 316**

- (Exam Topic 14)

Which of the following is the PRIMARY risk associated with Extensible Markup Language (XML) applications?

- A. Users can manipulate the code.
- B. The stack data structure cannot be replicated.
- C. The stack data structure is repetitive.
- D. Potential sensitive data leakage.

**Answer:** A

**NEW QUESTION 318**



- (Exam Topic 14)

If a content management system (CMC) is implemented, which one of the following would occur?

- A. Developers would no longer have access to production systems
- B. The applications placed into production would be secure
- C. Patching the systems would be completed more quickly
- D. The test and production systems would be running the same software

**Answer:** D

**NEW QUESTION 322**

- (Exam Topic 14)

Physical assets defined in an organization's Business Impact Analysis (BIA) could include which of the following?

- A. Personal belongings of organizational staff members
- B. Supplies kept off-site at a remote facility
- C. Cloud-based applications
- D. Disaster Recovery (DR) line-item revenues

**Answer:** B

**NEW QUESTION 325**

- (Exam Topic 14)

What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

- A. Mandatory Access Control (MAC)
- B. Discretionary Access Control (DAC)
- C. Role Based Access Control (RBAC)
- D. Attribute Based Access Control (ABAC)

**Answer:** D

**Explanation:**

Reference: [https://en.wikipedia.org/wiki/Attribute-based\\_access\\_control](https://en.wikipedia.org/wiki/Attribute-based_access_control)

**NEW QUESTION 330**

- (Exam Topic 14)

Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities?

- A. Definitions for each exposure type
- B. Vulnerability attack vectors
- C. Asset values for networks
- D. Exploit code metrics

**Answer:** C

**NEW QUESTION 332**

- (Exam Topic 14)

Functional security testing is MOST critical during which phase of the system development life cycle (SDLC)?

- A. Operations / Maintenance
- B. Implementation
- C. Acquisition / Development
- D. Initiation

**Answer:** B

**NEW QUESTION 336**

- (Exam Topic 14)

Additional padding may be added to the Encapsulating Security Protocol (ESP) trailer to provide which of the following?

- A. Access control
- B. Partial traffic flow confidentiality
- C. Protection against replay attack
- D. Data origin authentication

**Answer:** C

**NEW QUESTION 340**

- (Exam Topic 14)

Which of the following is a characteristic of covert security testing?

- A. Induces less risk than over testing
- B. Tests staff knowledge and Implementation of the organization's security policy
- C. Focuses on identifying vulnerabilities
- D. Tests and validates all security controls in the organization



**Answer:** B

**NEW QUESTION 345**

- (Exam Topic 14)

Which is the RECOMMENDED configuration mode for sensors for an intrusion prevention system (IPS) if the prevention capabilities will be used?

- A. Active
- B. Passive
- C. Inline
- D. Span

**Answer:** C

**NEW QUESTION 348**

- (Exam Topic 14)

During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should an assessor do?

- A. Increase the number and type of relevant staff to interview.
- B. Conduct a comprehensive examination of the Disaster Recovery Plan (DRP).
- C. Increase the level of detail of the interview questions.
- D. Conduct a detailed review of the organization's DR policy.

**Answer:** A

**NEW QUESTION 353**

- (Exam Topic 14)

When selecting a disk encryption technology, which of the following **MUST** also be assured to be encrypted?

- A. Master Boot Record (MBR)
- B. Pre-boot environment
- C. Basic Input Output System (BIOS)
- D. Hibernation file

**Answer:** A

**NEW QUESTION 356**

- (Exam Topic 14)

Which of the following job functions **MUST** be separated to maintain data and application integrity?

- A. Applications development and systems analysis
- B. Production control and data control functions
- C. Scheduling and computer operations
- D. Systems development and systems maintenance

**Answer:** D

**NEW QUESTION 357**

- (Exam Topic 14)

What is the **MOST** effective way to protect privacy?

- A. Eliminate or reduce collection of personal information.
- B. Encrypt all collected personal information.
- C. Classify all personal information at the highest information classification level.
- D. Apply tokenization to all personal information records.

**Answer:** D

**NEW QUESTION 359**

- (Exam Topic 14)

Which type of fire alarm system sensor is intended to detect fire at its earliest stage?

- A. Ionization
- B. Infrared
- C. Thermal
- D. Photoelectric

**Answer:** A

**NEW QUESTION 364**

- (Exam Topic 14)

If virus infection is suspected, which of the following is the **FIRST** step for the user to take?

- A. Unplug the computer from the network.
- B. Save the opened files and shutdown the computer.
- C. Report the incident to service desk.

D. Update the antivirus to the latest version.

**Answer:** C

**NEW QUESTION 369**

- (Exam Topic 14)

Which of the following models uses unique groups contained in unique conflict classes?

- A. Chinese Wall
- B. Bell-LaPadula
- C. Clark-Wilson
- D. Biba

**Answer:** C

**NEW QUESTION 374**

- (Exam Topic 14)

In fault-tolerant systems, what do rollback capabilities permit?

- A. Restoring the system to a previous functional state
- B. Identifying the error that caused the problem
- C. Allowing the system to an in a reduced manner
- D. Isolating the error that caused the problem

**Answer:** A

**NEW QUESTION 377**

- (Exam Topic 14)

Which of the following is the MOST important reason for timely installation of software patches?

- A. Attackers may be conducting network analysis.
- B. Patches are only available for a specific time.
- C. Attackers reverse engineer the exploit from the patch.
- D. Patches may not be compatible with proprietary software

**Answer:** C

**NEW QUESTION 381**

- (Exam Topic 14)

Utilizing a public wireless Local Area network (WLAN) to connect to a private network should be done only in which of the following situations?

- A. Extensible Authentication Protocol (EAP) is utilized to authenticate the user.
- B. The client machine has a personal firewall and utilizes a Virtual Private Network (VPN) to connect to the network.
- C. The client machine has antivirus software and has been seamed to determine if unauthorized ports are open.
- D. The wireless Access Point (AP) is placed in the internal private network.

**Answer:** A

**NEW QUESTION 382**

- (Exam Topic 14)

Which of the following initiates the systems recovery phase of a disaster recovery plan?

- A. Issuing a formal disaster declaration
- B. Activating the organization's hot site
- C. Evacuating the disaster site
- D. Assessing the extent of damage following the disaster

**Answer:** A

**NEW QUESTION 386**

- (Exam Topic 14)

Which of the following authorization standards is built to handle Application programming Interface (API) access for federated Identity management (FIM)?

- A. Remote Authentication Dial-In User Service (RADIUS)
- B. Terminal Access Controller Access Control System Plus (TACACS+)
- C. Open Authentication (OAuth)
- D. Security Assertion Markup Language (SAML)

**Answer:** C

**NEW QUESTION 389**

- (Exam Topic 14)

Assume that a computer was powered off when an information security professional arrived at a crime scene. Which of the following actions should be performed after the crime scene is isolated?

- A. Turn the computer on and collect volatile data.
- B. Turn the computer on and collect network information.
- C. Leave the computer off and prepare the computer for transportation to the laboratory
- D. Remove the hard drive, prepare it for transportation, and leave the hardware ta the scene.

**Answer:** C

**NEW QUESTION 392**

- (Exam Topic 14)

Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device Which has stolen?

- A. Whole device encryption with key escrow
- B. Mobile Device Management (MDMJ with device wipe
- C. Mobile device tracking with geolocation
- D. Virtual Private Network (VPN) with traffic encryption

**Answer:** B

**NEW QUESTION 395**

- (Exam Topic 14)

Which is the second phase of public key Infrastructure (pk1) key/certificate life-cycle management?

- A. Issued Phase
- B. Cancellation Phase
- C. Implementation phase
- D. Initialization Phase

**Answer:** C

**NEW QUESTION 396**

- (Exam Topic 14)

Which of the following is a characteristic of a challenge/response authentication process?

- A. Presenting distorted graphics of text for authentication
- B. Transmitting a hash based on the user's password
- C. Using a password history blacklist
- D. Requiring the use of non-consecutive numeric characters

**Answer:** A

**NEW QUESTION 400**

- (Exam Topic 14)

What is the best way for mutual authentication of devices belonging to the same organization?

- A. Token
- B. Certificates
- C. User ID and passwords
- D. Biometric

**Answer:** A

**Explanation:**

Reference: <https://books.google.com.pk/books?id=bb0re6h8JPAC&pg=PA637&lpg=PA637&dq=CISSP+for+mutual+auth>

**NEW QUESTION 402**

- (Exam Topic 14)

Which of the following will help identify the source internet protocol (IP) address of malware being exected on a computer?

- A. List of open network connections
- B. Display Transmission Control Protocol/Internet Protocol (TCP/IP) network configuration information.
- C. List of running processes
- D. Display the Address Resolution Protocol (APP) table.

**Answer:** A

**NEW QUESTION 403**

- (Exam Topic 14)

When designing on Occupent Emergency plan (OEP) for United states (US) Federal government facilities, what factor must be considered?

- A. location of emergency exits in building
- B. Average age of the agency employees
- C. Geographical location and structural design of building
- D. Federal agency for which plan is being drafted

**Answer:** A

**NEW QUESTION 406**

- (Exam Topic 14)

Change management policies and procedures belong to which of the following types of controls?

- A. Directive
- B. Detective
- C. Corrective
- D. Preventative

**Answer:** A

**Explanation:**

Reference: <https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Change+mana>

**NEW QUESTION 408**

- (Exam Topic 14)

Which type of test suite should be run for fast feedback during application development?

- A. Full recession
- B. End-to-end
- C. Smoke
- D. Specific functionality

**Answer:** C

**NEW QUESTION 413**

- (Exam Topic 14)

Which of the following is the PRIMARY security consideration for how an organization should handle Information Technology (IT) assets?

- A. The monetary value of the asset
- B. The controls implemented on the asset
- C. The physical form factor of the asset
- D. The classification of the data on the asset

**Answer:** D

**NEW QUESTION 418**

- (Exam Topic 14)

Which of the following is PRIMARILY adopted for ensuring the integrity of information is preserved?

- A. Data at rest protection
- B. Transport Layer Security (TLS)
- C. Role Based Access Control (RBAC)
- D. One-way encryption

**Answer:** A

**NEW QUESTION 422**

- (Exam Topic 14)

Which would result in the GREATEST impact following a breach to a cloud environment?

- A. The hypervisor host is poorly secured
- B. The same Logical Unit Number (LLN) is used for all VMs
- C. Insufficient network segregation
- D. Insufficient hardening of Virtual Machines (VM)

**Answer:** C

**NEW QUESTION 423**

- (Exam Topic 14)

Which of the following techniques is MOST useful when dealing with Advanced persistent Threat (APT) intrusions on live virtualized environments?

- A. Antivirus operations
- B. Reverse engineering
- C. Memory forensics
- D. Logfile analysis

**Answer:** B

**NEW QUESTION 427**

- (Exam Topic 14)

An Intrusion Detection System (IDS) is based on the general hypothesis that a security violation is associated with a pattern of system usage which can be

- A. differentiated from a normal usage pattern.
- B. used to detect known violations.
- C. used to detect a masquerader.

D. differentiated to detect all security violations.

**Answer:** A

**NEW QUESTION 430**

- (Exam Topic 14)

Which of the following is the MOST significant benefit to implementing a third-party federated identity architecture?

- A. Attribute assertions as agencies can request a larger set of attributes to fulfill service delivery
- B. Data decrease related to storing personal information
- C. Reduction in operational costs to the agency
- D. Enable business objectives so departments can focus on mission rather than the business of identitymanagement

**Answer:** C

**NEW QUESTION 431**

- (Exam Topic 14)

What is maintained by using write blocking devices when forensic evidence is examined?

- A. Inventory
- B. Integrity
- C. Confidentiality
- D. Availability

**Answer:** B

**NEW QUESTION 435**

- (Exam Topic 14)

What technique used for spoofing the origin of an email can successfully conceal the sender's Internet Protocol (IP) address?

- A. Change In-Reply-To data
- B. Web crawling
- C. Onion routing
- D. Virtual Private Network (VPN)

**Answer:** C

**NEW QUESTION 437**

- (Exam Topic 14)

Which of the following techniques BEST prevents buffer overflows?

- A. Boundary and perimeter offset
- B. Character set encoding
- C. Code auditing
- D. Variant type and bit length

**Answer:** B

**Explanation:**

Some products installed on systems can also watch for input values that might result in buffer overflows, but the best countermeasure is proper programming. This means use bounds checking. If an input value is only supposed to be nine characters, then the application should only accept nine characters and no more. Some languages are more susceptible to buffer overflows than others, so programmers should understand these issues, use the right languages for the right purposes, and carry out code review to identify buffer overflow vulnerabilities.

**NEW QUESTION 440**

- (Exam Topic 14)

Which attack defines a piece of code that is inserted into software to trigger a malicious function?

- A. Phishing
- B. Salami
- C. Back door
- D. Logic bomb

**Answer:** D

**NEW QUESTION 443**

- (Exam Topic 14)

Which of the following provides the BEST method to verify that security baseline configurations are maintained?

- A. Perform regular system security testing.
- B. Design security early in the development cycle.
- C. Analyze logs to determine user activities.
- D. Perform quarterly risk assessments.

**Answer:** A

**NEW QUESTION 447**

- (Exam Topic 14)

Which of the following in the BEST way to reduce the impact of an externally sourced flood attack?

- A. Stock the source address at the firewall.
- B. Have this service provide block the source address.
- C. Block all inbound traffic until the flood ends.
- D. Have the source service provider block the address

**Answer:** A

**NEW QUESTION 449**

- (Exam Topic 14)

When conducting a forensic criminal investigation on a computer hard drive, what should be done PRIOR to analysis?

- A. Create a backup copy of all the important files on the drive.
- B. Power off the computer and wait for assistance.
- C. Create a forensic image of the hard drive.
- D. Install forensic analysis software.

**Answer:** C

**NEW QUESTION 452**

- (Exam Topic 14)

In the common criteria (CC) for information technology (IT) security evaluation, increasing Evaluation Assurance Levels (EAL) results in which of the following?

- A. Increased functionality
- B. Increased interoperability
- C. Increase in resource requirement
- D. Increase in evaluated systems

**Answer:** B

**NEW QUESTION 455**

- (Exam Topic 14)

Which of the following attributes could be used to describe a protection mechanism of an open design methodology?

- A. It must be tamperproof to protect it from malicious attacks.
- B. It can facilitate independent confirmation of the design security.
- C. It can facilitate blackbox penetration testing.
- D. It exposes the design to vulnerabilities and malicious attacks.

**Answer:** A

**NEW QUESTION 460**

- (Exam Topic 14)

As a security manager which of the following is the MOST effective practice for providing value to an organization?

- A. Assess business risk and apply security resources accordingly
- B. Coordinate security implementations with internal audit
- C. Achieve compliance regardless of related technical issues
- D. Identify confidential information and protect it

**Answer:** D

**NEW QUESTION 463**

- (Exam Topic 14)

Which of the following processes has the PRIMARY purpose of identifying outdated software versions, missing patches, and lapsed system updates?

- A. Penetration testing
- B. Vulnerability management
- C. Software Development Life Cycle (SDLC)
- D. Life cycle management

**Answer:** B

**Explanation:**

Reference:

<https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/vulnerab>

**NEW QUESTION 467**

- (Exam Topic 14)

Which of the following is the weakest form of protection for an application that handles Personally Identifiable Information (PII)?

- A. Transport Layer Security (TLS)
- B. Ron Rivest Cipher 4 (RC4) encryption



- C. Security Assertion Markup Language (SAML)
- D. Multifactor authentication

**Answer:** B

**NEW QUESTION 468**

- (Exam Topic 14)

What does the term “100-year floodplain” mean to emergency preparedness officials?

- A. The area is expected to be safe from flooding for at least 100 years.
- B. The odds of a flood at this level are 1 in 100 in any given year.
- C. The odds are that the next significant flood will hit within the next 100 years.
- D. The last flood of any kind to hit the area was more than 100 years ago.

**Answer:** B

**NEW QUESTION 472**

- (Exam Topic 13)

Which one of the following is an advantage of an effective release control strategy form a configuration control standpoint?

- A. Ensures that a trace for all deliverables is maintained and auditable
- B. Enforces backward compatibility between releases
- C. Ensures that there is no loss of functionality between releases
- D. Allows for future enhancements to existing features

**Answer:** A

**NEW QUESTION 475**

- (Exam Topic 13)

Which of the following is the MOST common method of memory protection?

- A. Compartmentalization
- B. Segmentation
- C. Error correction
- D. Virtual Local Area Network (VLAN) tagging

**Answer:** B

**NEW QUESTION 476**

- (Exam Topic 13)

When developing a business case for updating a security program, the security program owner MUST do which of the following?

- A. Identify relevant metrics
- B. Prepare performance test reports
- C. Obtain resources for the security program
- D. Interview executive management

**Answer:** A

**NEW QUESTION 477**

- (Exam Topic 13)

Access to which of the following is required to validate web session management?

- A. Log timestamp
- B. Live session traffic
- C. Session state variables
- D. Test scripts

**Answer:** B

**NEW QUESTION 478**

- (Exam Topic 13)

A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report. In which phase of the assessment was this error MOST likely made?

- A. Enumeration
- B. Reporting
- C. Detection
- D. Discovery

**Answer:** A

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 481**

- (Exam Topic 13)

Who would be the BEST person to approve an organizations information security policy?

- A. Chief Information Officer (CIO)
- B. Chief Information Security Officer (CISO)
- C. Chief internal auditor
- D. Chief Executive Officer (CEO)

**Answer:** B

**Explanation:**

Section: Security Operations

**NEW QUESTION 483**

- (Exam Topic 13)

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

<u>Actions</u>		<u>Steps</u>
Define the perimeter.		Step 1
Identify the vulnerability.		Step 2
Assess the risk.		Step 3
Determine the actions.		Step 4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<u>Actions</u>		<u>Steps</u>
Define the perimeter.	Identify the vulnerability.	Step 1
Identify the vulnerability.	Define the perimeter.	Step 2
Assess the risk.	Assess the risk.	Step 3
Determine the actions.	Determine the actions.	Step 4

**NEW QUESTION 487**

- (Exam Topic 13)

Which of the following is the MOST important security goal when performing application interface testing?

- A. Confirm that all platforms are supported and function properly
- B. Evaluate whether systems or components pass data and control correctly to one another
- C. Verify compatibility of software, hardware, and network connections
- D. Examine error conditions related to external interfaces to prevent application details leakage

**Answer:** B

**NEW QUESTION 492**

- (Exam Topic 13)

Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

- A. Application proxy

- B. Port filter
- C. Network boundary router
- D. Access layer switch

**Answer:** D

**NEW QUESTION 496**

- (Exam Topic 13)

What is the BEST location in a network to place Virtual Private Network (VPN) devices when an internal review reveals network design flaws in remote access?

- A. In a dedicated Demilitarized Zone (DMZ)
- B. In its own separate Virtual Local Area Network (VLAN)
- C. At the Internet Service Provider (ISP)
- D. Outside the external firewall

**Answer:** B

**NEW QUESTION 500**

- (Exam Topic 13)

Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).

Which of the following represents a valid measure to help protect the network against unauthorized access?

- A. Implement path management
- B. Implement port based security through 802.1x
- C. Implement DHCP to assign IP address to server systems
- D. Implement change management

**Answer:** B

**NEW QUESTION 504**

- (Exam Topic 13)

A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements.

Which of the following BEST minimizes the risk of this happening again?

- A. Define additional security controls directly after the merger
- B. Include a procurement officer in the merger team
- C. Verify all contracts before a merger occurs
- D. Assign a compliancy officer to review the merger conditions

**Answer:** D

**NEW QUESTION 508**

- (Exam Topic 13)

Which of the following MUST be in place to recognize a system attack?

- A. Stateful firewall
- B. Distributed antivirus
- C. Log analysis
- D. Passive honeypot

**Answer:** C

**NEW QUESTION 511**

- (Exam Topic 13)

Which of the following would an attacker BEST be able to accomplish through the use of Remote Access Tools (RAT)?

- A. Reduce the probability of identification
- B. Detect further compromise of the target
- C. Destabilize the operation of the host
- D. Maintain and expand control

**Answer:** D

**NEW QUESTION 515**

- (Exam Topic 13)

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

- A. Mutual authentication
- B. Server authentication
- C. User authentication
- D. Streaming ciphertext data

**Answer:** C

**NEW QUESTION 518**

- (Exam Topic 13)

Which of the following is the BEST reason for writing an information security policy?

- A. To support information security governance
- B. To reduce the number of audit findings
- C. To deter attackers
- D. To implement effective information security controls

**Answer:** A

**NEW QUESTION 522**

- (Exam Topic 13)

The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. Which elements are required?

- A. Users, permissions, operations, and protected objects
- B. Roles, accounts, permissions, and protected objects
- C. Users, roles, operations, and protected objects
- D. Roles, operations, accounts, and protected objects

**Answer:** C

**NEW QUESTION 525**

- (Exam Topic 13)

Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

- A. Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.
- B. Maintaining segregation of duties.
- C. Standardized configurations for logging, alerting, and security metrics.
- D. Availability of security teams at the end of design process to perform last-minute manual audits and reviews.

**Answer:** B

**NEW QUESTION 528**

- (Exam Topic 13)

At a MINIMUM, audits of permissions to individual or group accounts should be scheduled

- A. annually
- B. to correspond with staff promotions
- C. to correspond with terminations
- D. continually

**Answer:** A

**NEW QUESTION 531**

- (Exam Topic 13)

A control to protect from a Denial-of-Service (DoS) attack has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

- A. 25%
- B. 50%
- C. 75%
- D. 100%

**Answer:** B

**NEW QUESTION 532**

- (Exam Topic 13)

Which of the following is the MOST challenging issue in apprehending cyber criminals?

- A. They often use sophisticated method to commit a crime.
- B. It is often hard to collect and maintain integrity of digital evidence.
- C. The crime is often committed from a different jurisdiction.
- D. There is often no physical evidence involved.

**Answer:** C

**NEW QUESTION 537**

- (Exam Topic 13)

In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

- A. Modifying source code without approval
- B. Promoting programs to production without approval
- C. Developers checking out source code without approval
- D. Developers using Rapid Application Development (RAD) methodologies without approval

**Answer:** A

**NEW QUESTION 538**

- (Exam Topic 13)

Which of the following is a characteristic of an internal audit?

- A. An internal audit is typically shorter in duration than an external audit.
- B. The internal audit schedule is published to the organization well in advance.
- C. The internal auditor reports to the Information Technology (IT) department
- D. Management is responsible for reading and acting upon the internal audit results

**Answer:** D

**NEW QUESTION 543**

- (Exam Topic 13)

Unused space in a disk cluster is important in media analysis because it may contain which of the following?

- A. Residual data that has not been overwritten
- B. Hidden viruses and Trojan horses
- C. Information about the File Allocation table (FAT)
- D. Information about patches and upgrades to the system

**Answer:** A

**NEW QUESTION 547**

- (Exam Topic 13)

Which of the following is MOST effective in detecting information hiding in Transmission Control Protocol/internet Protocol (TCP/IP) traffic?

- A. Stateful inspection firewall
- B. Application-level firewall
- C. Content-filtering proxy
- D. Packet-filter firewall

**Answer:** A

**NEW QUESTION 551**

- (Exam Topic 13)

As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

- A. Use a web scanner to scan for vulnerabilities within the website.
- B. Perform a code review to ensure that the database references are properly addressed.
- C. Establish a secure connection to the web server to validate that only the approved ports are open.
- D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

**Answer:** D

**NEW QUESTION 555**

- (Exam Topic 13)

Which of the BEST internationally recognized standard for evaluating security products and systems?

- A. Payment Card Industry Data Security Standards (PCI-DSS)
- B. Common Criteria (CC)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. Sarbanes-Oxley (SOX)

**Answer:** B

**NEW QUESTION 558**

- (Exam Topic 13)

Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

- A. identity provisioning
- B. access recovery
- C. multi-factor authentication (MFA)
- D. user access review

**Answer:** A

**NEW QUESTION 563**

- (Exam Topic 13)

An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?

- A. Diffie-Hellman (DH) algorithm
- B. Elliptic Curve Cryptography (ECC) algorithm

- C. Digital Signature algorithm (DSA)
- D. Rivest-Shamir-Adleman (RSA) algorithm

**Answer:** D

#### NEW QUESTION 566

- (Exam Topic 13)

An organization plan on purchasing a custom software product developed by a small vendor to support its business model. Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?

- A. A source code escrow clause
- B. Right to request an independent review of the software source code
- C. Due diligence form requesting statements of compliance with security requirements
- D. Access to the technical documentation

**Answer:** B

#### NEW QUESTION 570

- (Exam Topic 13)

Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

- A. Inert gas fire suppression system
- B. Halon gas fire suppression system
- C. Dry-pipe sprinklers
- D. Wet-pipe sprinklers

**Answer:** A

#### NEW QUESTION 571

- (Exam Topic 13)

Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

- A. Configuration
- B. Identity
- C. Compliance
- D. Patch

**Answer:** A

#### NEW QUESTION 575

- (Exam Topic 13)

What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

- A. The IDS can detect failed administrator logon attempts from servers.
- B. The IDS can increase the number of packets to analyze.
- C. The firewall can increase the number of packets to analyze.
- D. The firewall can detect failed administrator login attempts from servers

**Answer:** A

#### NEW QUESTION 579

- (Exam Topic 13)

What is the expected outcome of security awareness in support of a security awareness program?

- A. Awareness activities should be used to focus on security concerns and respond to those concerns accordingly
- B. Awareness is not an activity or part of the training but rather a state of persistence to support the program
- C. Awareness is trainin
- D. The purpose of awareness presentations is to broaden attention of security.
- E. Awareness is not trainin
- F. The purpose of awareness presentation is simply to focus attention on security.

**Answer:** C

#### NEW QUESTION 581

- (Exam Topic 13)

Drag the following Security Engineering terms on the left to the BEST definition on the right.



<u>Security Engineering Term</u>	<u>Definition</u>
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment	The method used to identify feasible security risk mitigation options and plans.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

**NEW QUESTION 582**

- (Exam Topic 13)

A company receives an email threat informing of an Imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques BEST addresses that threat?

- A. Deploying load balancers to distribute inbound traffic across multiple data centers
- B. Set Up Web Application Firewalls (WAFs) to filter out malicious traffic
- C. Implementing reverse web-proxies to validate each new inbound connection
- D. Coordinate with and utilize capabilities within Internet Service Provider (ISP)

**Answer:** D

**NEW QUESTION 586**

- (Exam Topic 13)

The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

- A. Application authentication
- B. Input validation
- C. Digital signing
- D. Device encryption

**Answer:** B

**NEW QUESTION 591**

- (Exam Topic 13)

Attack trees are MOST useful for which of the following?

- A. Determining system security scopes
- B. Generating attack libraries
- C. Enumerating threats
- D. Evaluating Denial of Service (DoS) attacks

**Answer:** C

**NEW QUESTION 596**

- (Exam Topic 12)

An organization's information security strategic plan MUST be reviewed

- A. whenever there are significant changes to a major application.

- B. quarterly, when the organization's strategic plan is updated.
- C. whenever there are major changes to the business.
- D. every three years, when the organization's strategic plan is updated.

**Answer:** C

**NEW QUESTION 598**

- (Exam Topic 12)

Which of the following information **MUST** be provided for user account provisioning?

- A. Full name
- B. Unique identifier
- C. Security question
- D. Date of birth

**Answer:** B

**NEW QUESTION 603**

- (Exam Topic 12)

The **PRIMARY** purpose of accreditation is to:

- A. comply with applicable laws and regulations.
- B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
- C. protect an organization's sensitive data.
- D. verify that all security controls have been implemented properly and are operating in the correct manner.

**Answer:** B

**NEW QUESTION 607**

- (Exam Topic 12)

Which of the following would **BEST** describe the role directly responsible for data within an organization?

- A. Data custodian
- B. Information owner
- C. Database administrator
- D. Quality control

**Answer:** A

**NEW QUESTION 608**

- (Exam Topic 12)

Which of the following approaches is the **MOST** effective way to dispose of data on multiple hard drives?

- A. Delete every file on each drive.
- B. Destroy the partition table for each drive using the command line.
- C. Degauss each drive individually.
- D. Perform multiple passes on each drive using approved formatting methods.

**Answer:** D

**NEW QUESTION 611**

- (Exam Topic 12)

When evaluating third-party applications, which of the following is the **GREATEST** responsibility of Information Security?

- A. Accept the risk on behalf of the organization.
- B. Report findings to the business to determine security gaps.
- C. Quantify the risk to the business for product selection.
- D. Approve the application that best meets security requirements.

**Answer:** C

**NEW QUESTION 616**

- (Exam Topic 12)

Which of the following is the **MOST** important goal of information asset valuation?

- A. Developing a consistent and uniform method of controlling access on information assets
- B. Developing appropriate access control policies and guidelines
- C. Assigning a financial value to an organization's information assets
- D. Determining the appropriate level of protection

**Answer:** D

**NEW QUESTION 620**

- (Exam Topic 12)

Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

- A. Transference
- B. Covert channel
- C. Bleeding
- D. Cross-talk

**Answer:** D

**NEW QUESTION 621**

- (Exam Topic 12)

A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

- A. Enterprise asset management framework
- B. Asset baseline using commercial off the shelf software
- C. Asset ownership database using domain login records
- D. A script to report active user logins on assets

**Answer:** A

**NEW QUESTION 626**

- (Exam Topic 12)

When using Generic Routing Encapsulation (GRE) tunneling over Internet Protocol version 4 (IPv4), where is the GRE header inserted?

- A. Into the options field
- B. Between the delivery header and payload
- C. Between the source and destination addresses
- D. Into the destination address

**Answer:** B

**NEW QUESTION 628**

- (Exam Topic 12)

What is an advantage of Elliptic Curve Cryptography (ECC)?

- A. Cryptographic approach that does not require a fixed-length key
- B. Military-strength security that does not depend upon secrecy of the algorithm
- C. Opportunity to use shorter keys for the same level of security
- D. Ability to use much longer keys for greater security

**Answer:** C

**NEW QUESTION 632**

- (Exam Topic 12)

Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

- A. To verify that only employees have access to the facility.
- B. To identify present hazards requiring remediation.
- C. To monitor staff movement throughout the facility.
- D. To provide a safe environment for employees.

**Answer:** D

**NEW QUESTION 635**

- (Exam Topic 12)

Which of the following BEST represents the concept of least privilege?

- A. Access to an object is denied unless access is specifically allowed.
- B. Access to an object is only available to the owner.
- C. Access to an object is allowed unless it is protected by the information security policy.
- D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

**Answer:** A

**NEW QUESTION 637**

- (Exam Topic 12)

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

- A. Revoke access temporarily.
- B. Block user access and delete user account after six months.
- C. Block access to the offices immediately.
- D. Monitor account usage temporarily.

**Answer:** D

**NEW QUESTION 640**

- (Exam Topic 12)

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

- A. Asset Management, Business Environment, Governance and Risk Assessment
- B. Access Control, Awareness and Training, Data Security and Maintenance
- C. Anomalies and Events, Security Continuous Monitoring and Detection Processes
- D. Recovery Planning, Improvements and Communications

**Answer:** A

#### NEW QUESTION 645

- (Exam Topic 12)

What is the BEST way to encrypt web application communications?

- A. Secure Hash Algorithm 1 (SHA-1)
- B. Secure Sockets Layer (SSL)
- C. Cipher Block Chaining Message Authentication Code (CBC-MAC)
- D. Transport Layer Security (TLS)

**Answer:** D

#### NEW QUESTION 649

- (Exam Topic 12)

Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

- A. The dynamic reconfiguration of systems
- B. The cost of downtime
- C. A recovery strategy for all business processes
- D. A containment strategy

**Answer:** C

#### NEW QUESTION 651

- (Exam Topic 11)

What is one way to mitigate the risk of security flaws in custom software?

- A. Include security language in the Earned Value Management (EVM) contract
- B. Include security assurance clauses in the Service Level Agreement (SLA)
- C. Purchase only Commercial Off-The-Shelf (COTS) products
- D. Purchase only software with no open source Application Programming Interfaces (APIs)

**Answer:** B

#### NEW QUESTION 656

- (Exam Topic 12)

Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

<u>Access Control Type</u>	<u>Example</u>
Administrative	Labeling of sensitive data
Technical	Biometrics for authentication
Logical	Constrained user interface
Physical	Radio Frequency Identification (RFID) badge

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Administrative – labeling of sensitive data  
 Technical – Constrained user interface  
 Logical – Biometrics for authentication  
 Physical – Radio Frequency Identification (RFID) badge

#### NEW QUESTION 661

- (Exam Topic 11)

What security risk does the role-based access approach mitigate MOST effectively?

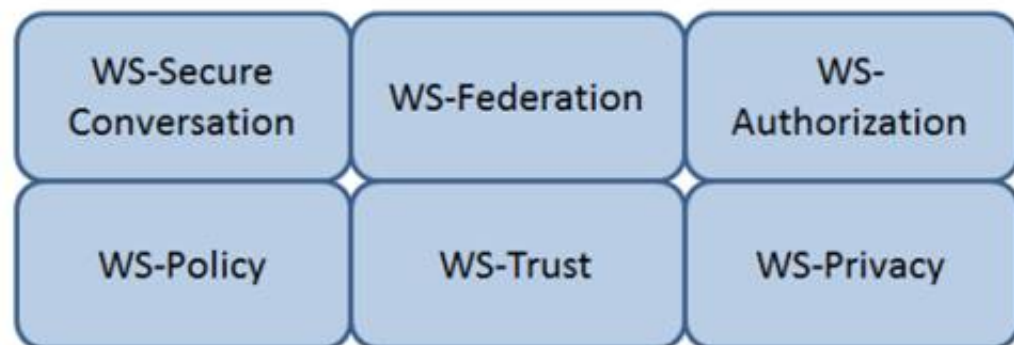
- A. Excessive access rights to systems and data
- B. Segregation of duties conflicts within business applications
- C. Lack of system administrator activity monitoring
- D. Inappropriate access requests

**Answer:** A

#### NEW QUESTION 664

- (Exam Topic 11)

Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

WS-Trust

The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.

Reference: <https://msdn.microsoft.com/en-us/library/ff650503.aspx>

#### NEW QUESTION 667

- (Exam Topic 11)

During a fingerprint verification process, which of the following is used to verify identity and authentication?

- A. A pressure value is compared with a stored template
- B. Sets of digits are matched with stored values
- C. A hash table is matched to a database of stored value
- D. A template of minutiae is compared with a stored template

**Answer:** D

#### NEW QUESTION 668

- (Exam Topic 11)

Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

- A. Delayed revocation or destruction of credentials
- B. Modification of Certificate Revocation List
- C. Unauthorized renewal or re-issuance
- D. Token use after decommissioning

**Answer:** B

#### NEW QUESTION 669

- (Exam Topic 11)

What is the PRIMARY difference between security policies and security procedures?

- A. Policies are used to enforce violations, and procedures create penalties
- B. Policies point to guidelines, and procedures are more contractual in nature
- C. Policies are included in awareness training, and procedures give guidance
- D. Policies are generic in nature, and procedures contain operational details

**Answer:** D

#### NEW QUESTION 670

- (Exam Topic 11)

Which of the following is a recommended alternative to an integrated email encryption system?



- A. Sign emails containing sensitive data
- B. Send sensitive data in separate emails
- C. Encrypt sensitive data separately in attachments
- D. Store sensitive information to be sent in encrypted drives

**Answer:** C

#### NEW QUESTION 675

- (Exam Topic 11)

Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

- A. dig
- B. ifconfig
- C. ipconfig
- D. nbtstat

**Answer:** A

#### NEW QUESTION 676

- (Exam Topic 11)

A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

- A. Public Key Infrastructure (PKI) and digital signatures
- B. Trusted server certificates and passphrases
- C. User ID and password
- D. Asymmetric encryption and User ID

**Answer:** A

#### NEW QUESTION 681

- (Exam Topic 11)

Which of the following is a function of Security Assertion Markup Language (SAML)?

- A. File allocation
- B. Redundancy check
- C. Extended validation
- D. Policy enforcement

**Answer:** D

#### NEW QUESTION 685

- (Exam Topic 11)

Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

- A. poor governance over security processes and procedures
- B. immature security controls and procedures
- C. variances against regulatory requirements
- D. unanticipated increases in security incidents and threats

**Answer:** A

#### NEW QUESTION 690

- (Exam Topic 11)

Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

- A. Hierarchical inheritance
- B. Dynamic separation of duties
- C. The Clark-Wilson security model
- D. The Bell-LaPadula security model

**Answer:** B

#### NEW QUESTION 695

- (Exam Topic 11)

What does an organization FIRST review to assure compliance with privacy requirements?

- A. Best practices
- B. Business objectives
- C. Legal and regulatory mandates
- D. Employee's compliance to policies and standards

**Answer:** C

#### NEW QUESTION 696



- (Exam Topic 11)

The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it

- A. exploits weak authentication to penetrate networks.
- B. can be detected with signature analysis.
- C. looks like normal network activity.
- D. is commonly confused with viruses or worms.

**Answer: C**

#### NEW QUESTION 698

- (Exam Topic 11)

Which of the following BEST describes a rogue Access Point (AP)?

- A. An AP that is not protected by a firewall
- B. An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data Encryption Algorithm (3DES)
- C. An AP connected to the wired infrastructure but not under the management of authorized network administrators
- D. An AP infected by any kind of Trojan or Malware

**Answer: C**

#### NEW QUESTION 703

- (Exam Topic 11)

While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

- A. They should be recycled to save energy.
- B. They should be recycled according to NIST SP 800-88.
- C. They should be inspected and sanitized following the organizational policy.
- D. They should be inspected and categorized properly to sell them for reuse.

**Answer: C**

#### NEW QUESTION 704

- (Exam Topic 11)

What is the process called when impact values are assigned to the security objectives for information types?

- A. Qualitative analysis
- B. Quantitative analysis
- C. Remediation
- D. System security categorization

**Answer: D**

#### NEW QUESTION 709

- (Exam Topic 11)

Which one of the following is a common risk with network configuration management?

- A. Patches on the network are difficult to keep current.
- B. It is the responsibility of the systems administrator.
- C. User ID and passwords are never set to expire.
- D. Network diagrams are not up to date.

**Answer: D**

#### NEW QUESTION 714

- (Exam Topic 11)

Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?

- A. Data at rest encryption
- B. Configuration Management
- C. Integrity checking software
- D. Cyclic redundancy check (CRC)

**Answer: D**

#### NEW QUESTION 719

- (Exam Topic 11)

Which of the following questions can be answered using user and group entitlement reporting?

- A. When a particular file was last accessed by a user
- B. Change control activities for a particular group of users
- C. The number of failed login attempts for a particular user
- D. Where does a particular user have access within the network

**Answer: D**

**NEW QUESTION 721**

- (Exam Topic 11)

The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the

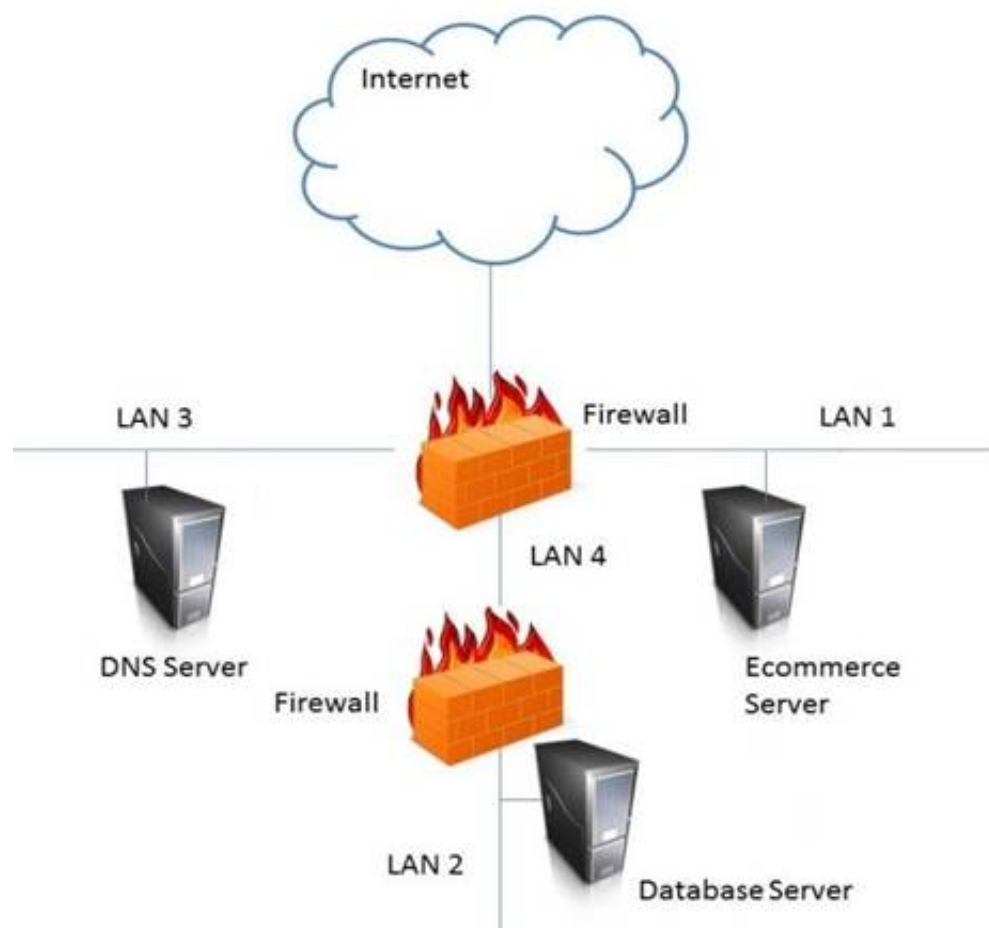
- A. right to refuse or permit commercial rentals.
- B. right to disguise the software's geographic origin.
- C. ability to tailor security parameters based on location.
- D. ability to confirm license authenticity of their works.

**Answer:** A

**NEW QUESTION 722**

- (Exam Topic 11)

In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

LAN 4

**NEW QUESTION 726**

- (Exam Topic 11)

What is the MOST effective method of testing custom application code?

- A. Negative testing
- B. White box testing
- C. Penetration testing
- D. Black box testing

**Answer:** B

**NEW QUESTION 727**

- (Exam Topic 11)

The BEST method to mitigate the risk of a dictionary attack on a system is to

- A. use a hardware token.
- B. use complex passphrases.
- C. implement password history.
- D. encrypt the access control list (ACL).

**Answer:** A

**NEW QUESTION 728**

- (Exam Topic 11)

Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

- A. Discretionary Access Control (DAC) procedures
- B. Mandatory Access Control (MAC) procedures
- C. Data link encryption
- D. Segregation of duties

**Answer:** D

**NEW QUESTION 730**

- (Exam Topic 11)

The 802.1x standard provides a framework for what?

- A. Network authentication for only wireless networks
- B. Network authentication for wired and wireless networks
- C. Wireless encryption using the Advanced Encryption Standard (AES)
- D. Wireless network encryption using Secure Sockets Layer (SSL)

**Answer:** B

**NEW QUESTION 731**

- (Exam Topic 11)

How does an organization verify that an information system's current hardware and software match the standard system configuration?

- A. By reviewing the configuration after the system goes into production
- B. By running vulnerability scanning tools on all devices in the environment
- C. By comparing the actual configuration of the system against the baseline
- D. By verifying all the approved security patches are implemented

**Answer:** C

**NEW QUESTION 733**

- (Exam Topic 11)

Which of the following is an advantage of on-premise Credential Management Systems?

- A. Improved credential interoperability
- B. Control over system configuration
- C. Lower infrastructure capital costs
- D. Reduced administrative overhead

**Answer:** B

**NEW QUESTION 736**

- (Exam Topic 10)

Refer to the information below to answer the question.

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.

If the intrusion causes the system processes to hang, which of the following has been affected?

- A. System integrity
- B. System availability
- C. System confidentiality
- D. System auditability

**Answer:** B

**NEW QUESTION 738**

- (Exam Topic 10)

The use of proximity card to gain access to a building is an example of what type of security control?

- A. Legal
- B. Logical
- C. Physical
- D. Procedural

**Answer:** C

**NEW QUESTION 740**

- (Exam Topic 10)

Which of the following actions **MUST** be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?

- A. Make changes following principle and design guidelines.
- B. Stop the application until the vulnerability is fixed.
- C. Report the vulnerability to product owner.
- D. Monitor the application and review code.

**Answer:** C

**NEW QUESTION 744**

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will MOST likely allow the organization to keep risk at an acceptable level?

- A. Increasing the amount of audits performed by third parties
- B. Removing privileged accounts from operational staff
- C. Assigning privileged functions to appropriate staff
- D. Separating the security function into distinct roles

**Answer: C**

**NEW QUESTION 749**

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

In addition to authentication at the start of the user session, best practice would require re-authentication

- A. periodically during a session.
- B. for each business process.
- C. at system sign-off.
- D. after a period of inactivity.

**Answer: D**

**NEW QUESTION 752**

- (Exam Topic 10)

Which of the following BEST describes Recovery Time Objective (RTO)?

- A. Time of data validation after disaster
- B. Time of data restoration from backup after disaster
- C. Time of application resumption after disaster
- D. Time of application verification after disaster

**Answer: C**

**NEW QUESTION 755**

- (Exam Topic 10)

When using third-party software developers, which of the following is the MOST effective method of providing software development Quality Assurance (QA)?

- A. Retain intellectual property rights through contractual wording.
- B. Perform overlapping code reviews by both parties.
- C. Verify that the contractors attend development planning meetings.
- D. Create a separate contractor development environment.

**Answer: B**

**NEW QUESTION 760**

- (Exam Topic 10)

Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

- A. Requirements Analysis
- B. Development and Deployment
- C. Production Operations
- D. Utilization Support

**Answer: A**

**NEW QUESTION 761**

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.

In addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?

- A. Text editors, database, and Internet phone applications
- B. Email, presentation, and database applications
- C. Image libraries, presentation and spreadsheet applications
- D. Email, media players, and instant messaging applications

**Answer: D**

**NEW QUESTION 766**

- (Exam Topic 10)

When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?

- A. Testing phase
- B. Development phase
- C. Requirements definition phase
- D. Operations and maintenance phase

**Answer: C**

#### NEW QUESTION 768

- (Exam Topic 10)

Which of the following is the MOST crucial for a successful audit plan?

- A. Defining the scope of the audit to be performed
- B. Identifying the security controls to be implemented
- C. Working with the system owner on new controls
- D. Acquiring evidence of systems that are not compliant

**Answer: A**

#### NEW QUESTION 770

- (Exam Topic 10)

For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

- A. Hash functions
- B. Data segregation
- C. File system permissions
- D. Non-repudiation controls

**Answer: B**

#### NEW QUESTION 772

- (Exam Topic 10)

What is the BEST method to detect the most common improper initialization problems in programming languages?

- A. Use and specify a strong character encoding.
- B. Use automated static analysis tools that target this type of weakness.
- C. Perform input validation on any numeric inputs by assuring that they are within the expected range.
- D. Use data flow analysis to minimize the number of false positives.

**Answer: B**

#### NEW QUESTION 776

- (Exam Topic 10)

A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

- A. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.
- B. Use Secure Sockets Layer (SSL) VPN technology.
- C. Use Secure Shell (SSH) with public/private keys.
- D. Require students to purchase home router capable of VPN.

**Answer: B**

#### NEW QUESTION 780

- (Exam Topic 10)

A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

- A. The inherent risk is greater than the residual risk.
- B. The Annualized Loss Expectancy (ALE) approaches zero.
- C. The expected loss from the risk exceeds mitigation costs.
- D. The infrastructure budget can easily cover the upgrade costs.

**Answer: C**

#### NEW QUESTION 783

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

What MUST the access control logs contain in addition to the identifier?

- A. Time of the access
- B. Security classification



- C. Denied access attempts
- D. Associated clearance

**Answer:** A

#### NEW QUESTION 788

- (Exam Topic 10)

A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

- A. The entire enterprise network infrastructure.
- B. The handheld devices, wireless access points and border gateway.
- C. The end devices, wireless access points, WLAN, switches, management console, and firewall.
- D. The end devices, wireless access points, WLAN, switches, management console, and Internet

**Answer:** C

#### NEW QUESTION 791

- (Exam Topic 9)

Which of the following is a network intrusion detection technique?

- A. Statistical anomaly
- B. Perimeter intrusion
- C. Port scanning
- D. Network spoofing

**Answer:** C

#### NEW QUESTION 792

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.

What is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?

- A. Client privilege administration is inherently weaker than server privilege administration.
- B. Client hardening and management is easier on clients than on servers.
- C. Client-based attacks are more common and easier to exploit than server and network based attacks.
- D. Client-based attacks have higher financial impact.

**Answer:** C

#### NEW QUESTION 797

- (Exam Topic 9)

Which one of the following considerations has the LEAST impact when considering transmission security?

- A. Network availability
- B. Data integrity
- C. Network bandwidth
- D. Node locations

**Answer:** C

#### NEW QUESTION 802

- (Exam Topic 9)

Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

- A. Encrypt and hash all PII to avoid disclosure and tampering.
- B. Store PII for no more than one year.
- C. Avoid storing PII in a Cloud Service Provider.
- D. Adherence to collection limitation laws and regulations.

**Answer:** D

#### NEW QUESTION 807

- (Exam Topic 9)

An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?

- A. A dictionary attack
- B. A Denial of Service (DoS) attack
- C. A spoofing attack
- D. A backdoor installation

**Answer:** A



**NEW QUESTION 809**

- (Exam Topic 9)

A practice that permits the owner of a data object to grant other users access to that object would usually provide

- A. Mandatory Access Control (MAC).
- B. owner-administered control.
- C. owner-dependent access control.
- D. Discretionary Access Control (DAC).

**Answer:** D

**NEW QUESTION 811**

- (Exam Topic 9)

What is the ultimate objective of information classification?

- A. To assign responsibility for mitigating the risk to vulnerable systems
- B. To ensure that information assets receive an appropriate level of protection
- C. To recognize that the value of any item of information may change over time
- D. To recognize the optimal number of classification categories and the benefits to be gained from their use

**Answer:** B

**NEW QUESTION 814**

- (Exam Topic 9)

In a basic SYN flood attack, what is the attacker attempting to achieve?

- A. Exceed the threshold limit of the connection queue for a given service
- B. Set the threshold to zero for a given service
- C. Cause the buffer to overflow, allowing root access
- D. Flush the register stack, allowing hijacking of the root account

**Answer:** A

**NEW QUESTION 819**

- (Exam Topic 9)

What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

- A. Man-in-the-Middle (MITM) attack
- B. Smurfing
- C. Session redirect
- D. Spoofing

**Answer:** D

**NEW QUESTION 823**

- (Exam Topic 9)

Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

- A. Network Address Translation (NAT)
- B. Application Proxy
- C. Routing Information Protocol (RIP) Version 2
- D. Address Masking

**Answer:** A

**NEW QUESTION 825**

- (Exam Topic 9)

Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

- A. Smurf
- B. Rootkit exploit
- C. Denial of Service (DoS)
- D. Cross site scripting (XSS)

**Answer:** D

**NEW QUESTION 829**

- (Exam Topic 9)

By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

- A. confidentiality of the traffic is protected.
- B. opportunity to sniff network traffic exists.
- C. opportunity for device identity spoofing is eliminated.
- D. storage devices are protected against availability attacks.

**Answer:** B

**NEW QUESTION 830**

- (Exam Topic 9)

Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

- A. Secure Sockets Layer (SSL) key exchange
- B. Internet Key Exchange (IKE)
- C. Security Key Exchange (SKE)
- D. Internet Control Message Protocol (ICMP)

**Answer: B**

**NEW QUESTION 835**

- (Exam Topic 9)

Which of the following is an appropriate source for test data?

- A. Production data that is secured and maintained only in the production environment.
- B. Test data that has no similarities to production data.
- C. Test data that is mirrored and kept up-to-date with production data.
- D. Production data that has been sanitized before loading into a test environment.

**Answer: D**

**NEW QUESTION 836**

- (Exam Topic 9)

What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

- A. Physical access to the electronic hardware
- B. Regularly scheduled maintenance process
- C. Availability of the network connection
- D. Processing delays

**Answer: A**

**NEW QUESTION 839**

- (Exam Topic 9)

Why MUST a Kerberos server be well protected from unauthorized access?

- A. It contains the keys of all clients.
- B. It always operates at root privilege.
- C. It contains all the tickets for services.
- D. It contains the Internet Protocol (IP) address of all network entities.

**Answer: A**

**NEW QUESTION 842**

- (Exam Topic 9)

Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?

- A. Anti-tampering
- B. Secure card reader
- C. Radio Frequency (RF) scanner
- D. Intrusion Prevention System (IPS)

**Answer: A**

**NEW QUESTION 846**

- (Exam Topic 9)

Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

- A. It uses a Subscriber Identity Module (SIM) for authentication.
- B. It uses encrypting techniques for all communications.
- C. The radio spectrum is divided with multiple frequency carriers.
- D. The signal is difficult to read as it provides end-to-end encryption.

**Answer: A**

**NEW QUESTION 850**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CISSP Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CISSP-dumps.html>