# CISSP

Number: CISSP
Passing Score: 800
Time Limit: 120 min
File Version: 1

CISSP


**Website:** https://vceplus.com
**VCE to PDF Converter:** https://vceplus.com/vce-to-pdf/
**Facebook:** https://www.facebook.com/VCE.For.All.VN/
**Twitter :** https://twitter.com/VCE_Plus

**https://vceplus.com/**

**Sections**

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing

7. Security Operations
8. Software Development Security
9. Mixed questions

**Exam A**

**QUESTION 1**
All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

A. determine the risk of a business interruption occurring
B. determine the technological dependence of the business processes


https://vceplus.com/

C. Identify the operational impacts of a business interruption
D. Identify the financial impacts of a business interruption

**Correct Answer:** B
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**
Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjbktbTpLaAhVIr48KHZuhB0UQFggmMAA&url=http%3A%2F%2Fwww.oregon.gov%2Fdas%2FProcurement%2FGuiddoc% 2FBusImpAnalysQs.doc&usg=AOvVaw1wBxcnLP8ceI_yhv2rsI9h

**QUESTION 2**
Which of the following represents the GREATEST risk to data confidentiality?

A. Network redundancies are not implemented

B. Security awareness training is not completed
C. Backup tapes are generated unencrypted
D. Users have administrative privileges

**Correct Answer:** C
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**
**QUESTION 3**
A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

A. Application
B. Storage
C. Power
D. Network

**Correct Answer:** C
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**
Reference: https://www.colocationamerica.com/data-center/tier-standards-overview.htm

**QUESTION 4**
When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

A. Only when assets are clearly defined
B. Only when standards are defined
C. Only when controls are put in place
D. Only procedures are defined

**Correct Answer:** A
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

A. Development, testing, and deployment
B. Prevention, detection, and remediation
C. People, technology, and operations
D. Certification, accreditation, and monitoring

**Correct Answer:** C
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**
Reference: https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165 (14)

**QUESTION 6**
A control to protect from a Denial-of-Service (DoS) attach 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%

**Correct Answer:** A
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

A. Security governance
B. Risk management
C. Security portfolio management
D. Risk assessment

**Correct Answer:** B
**Section: Security and Risk Management**
**Explanation**
**Explanation/Reference:**

**QUESTION 8**
Which of the following mandates the amount and complexity of security controls applied to a security risk?

A. Security vulnerabilities
B. Risk tolerance
C. Risk mitigation
D. Security staff

**Correct Answer:** C
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
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 minimize**s 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

**Correct Answer:** D

**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
Which of the following is a direct monetary cost of a security incident?

A. Morale
B. Reputation
C. Equipment D. Information

**Correct Answer:** C
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Which of the following would **MINIMIZE** the ability of an attacker to exploit a buffer overflow?

A. Memory review
B. Code review
C. Message division
D. Buffer division

**Correct Answer:** B
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Which of the following mechanisms will **BEST** prevent a Cross-Site Request Forgery (CSRF) attack?

A. parameterized database queries
B. whitelist input values
C. synchronized session tokens
D. use strong ciphers

**Correct Answer:** C
**Section: Security and Risk Management**
**Explanation**

**Explanation/Reference:**
**QUESTION 13**
Which of the following is MOST important when assigning ownership of an asset to a department?

A. The department should report to the business owner
B. Ownership of the asset should be periodically reviewed
C. Individual accountability should be ensured
D. All members should be trained on their responsibilities

**Correct Answer:** B
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
Which one of the following affects the classification of data?

A. Assigned security label
B. Multilevel Security (MLS) architecture
C. Minimum query size
D. Passage of time

**Correct Answer:** D
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Which of the following BEST describes the responsibilities of a data owner?

A. Ensuring quality and validation through periodic audits for ongoing data integrity
B. Maintaining fundamental data availability, including data storage and archiving
C. Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
D. Determining the impact the information has on the mission of the organization

**Correct Answer:** C
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**
Reference: http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/asset-security/data-and-system-ownership/#gref

**QUESTION 16**
In a data classification scheme, the data is owned by the

A. system security managers
B. business managers
C. Information Technology (IT) managers
D. end users

**Correct Answer:** B
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

A. Personal Identity Verification (PIV)
B. Cardholder Unique Identifier (CHUID) authentication

C. Physical Access Control System (PACS) repeated attempt detection
D. Asymmetric Card Authentication Key (CAK) challenge-response

**Correct Answer:** C
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Which factors **MUST** be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?
A. System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements
B. Data stewardship roles, data handling and storage standards, data lifecycle requirements
C. Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements
D. System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

**Correct Answer:** A
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
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. Diffle-Hellman (DH) algorithm
B. Elliptic Curve Cryptography (ECC) algorithm
C. Digital Signature algorithm (DSA)
D. Rivest-Shamir-Adleman (RSA) algorithm

**Correct Answer:** A
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
A company seizes a mobile device suspected of being used in committing fraud. What would be the **BEST** method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

A. Put the device in airplane mode
B. Suspend the account with the telecommunication provider
C. Remove the SIM card
D. Turn the device off

**Correct Answer:** A
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which of the following is the **MOST** effective method to mitigate Cross-Site Scripting (XSS) attacks?

A. Use Software as a Service (SaaS)
B. Whitelist input validation
C. Require client certificates
D. Validate data output

**Correct Answer:** B
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device.
Which of the following is **MOST** effective to mitigate future infections?

A. Develop a written organizational policy prohibiting unauthorized USB devices

B. Train users on the dangers of transferring data in USB devices C. Implement centralized technical control of USB port connections


https://vceplus.com/

D. Encrypt removable USB devices containing data at rest

**Correct Answer:** C
**Section: Asset Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

A. Hashing the data before encryption
B. Hashing the data after encryption
C. Compressing the data after encryption
D. Compressing the data before encryption

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

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

**Correct Answer:** D
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
Who in the organization is accountable for classification of data information assets?
A. Data owner
B. Data architect
C. Chief Information Security Officer (CISO)
D. Chief Information Officer (CIO)

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
A **minima**l implementation of endpoint security includes which of the following?

A. Trusted platforms
B. Host-based firewalls
C. Token-based authentication
D. Wireless Access Points (AP)

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
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 training. The purpose of awareness presentations is to broaden attention of security.
D. Awareness is not training. The purpose of awareness presentation is simply to focus attention on security.

**Correct Answer:** C
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
Which security modes is **MOST** commonly used in a commercial environment because it protects the integrity of financial and accounting data?

A. Biba
B. Graham-Denning
C. Clark-Wilson
D. Beil-LaPadula

**Correct Answer:** C
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
What is the foundation of cryptographic functions?

A. Encryption
B. Cipher

C. Hash
D. Entropy

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover. Which access control mechanism would be preferred?

Attribute Based Access Control (ABAC)

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

**Correct Answer:** D
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
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

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

A. Mandatory Access Control (MAC)
B. Access Control List (ACL)
C. Discretionary Access Control (DAC)
D. Authorized user control

**Correct Answer:** A

A.

**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following is a common characteristic of privacy?

A. Provision for maintaining an audit trail of access to the private data
B. Notice to the subject of the existence of a database containing relevant credit card data
C. Process for the subject to inspect and correct personal data on-site
D. Database requirements for integration of privacy data

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
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

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**

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

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.

**Correct Answer:** B
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results.
What should be implemented to **BEST** achieve the desired results?

A. Configuration Management Database (CMDB)

B. Source code repository

C. Configuration Management Plan (CMP)

D. System performance monitoring application

**Correct Answer:** C
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
Which of the following is a responsibility of a data steward?

A. Ensure alignment of the data governance effort to the organization.

B. Conduct data governance interviews with the organization.

C. Document data governance requirements.

A.

D. Ensure that data decisions and impacts are communicated to the organization.

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Which security approach will **BEST** minimize Personally Identifiable Information (PII) loss from a data breach?

A. End-to-end data encryption for data in transit
B. Continuous monitoring of potential vulnerabilities
C. A strong breach notification process
D. Limited collection of individuals' confidential data

**Correct Answer:** D
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Sensitive customer data is going to be added to a database. What is the **MOST** effective implementation for ensuring data privacy?

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

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which of the following is the **BEST** reason for writing an information security policy?

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

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
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)

**Correct Answer:** B
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

A. Truncating parts of the data
B. Applying Access Control Lists (ACL) to the data
C. Appending non-watermarked data to watermarked data
D. Storing the data in a database

A.

**Correct Answer:** A
**Section: Security Architecture and Engineering**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

A. Layer 2 Tunneling Protocol (L2TP)
B. Link Control Protocol (LCP)
C. Challenge Handshake Authentication Protocol (CHAP)
D. Packet Transfer Protocol (PTP)

**Correct Answer:** B
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

A. Packet filtering
B. Port services filtering
C. Content filtering
D. Application access control

**Correct Answer:** A
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**
Reference: https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309 (10)

**QUESTION 45**
An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

A. Add a new rule to the application layer firewall
B. Block access to the service
C. Install an Intrusion Detection System (IDS)

D. Patch the application source code

**Correct Answer:** A
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 46**
A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.
Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

A. Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.
B. Gratuitous ARP requires the use of insecure layer 3 protocols.
C. Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.
D. Gratuitous ARP requires the risk of a Man-in-the-Middle (MITM) attack.

**Correct Answer:** D
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 47**
Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

A. Transport layer handshake compression
B. Application layer negotiation
C. Peer identity authentication
D. Digital certificate revocation

**Correct Answer:** C
**Section: Communication and Network Security**
**Explanation**
**QUESTION 48**

**Explanation/Reference:**

A chemical plan wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade. Which of the following is the **GREATEST** impact on security for the network?

A. The network administrators have no knowledge of ICS
B. The ICS is now accessible from the office network
C. The ICS does not support the office password policy
D. RS422 is more reliable than Ethernet

**Correct Answer:** B
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 49**
What does a Synchronous (SYN) flood attack do?

A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state
B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

**Correct Answer:** B
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 50**
Which of the following is considered best practice for preventing e-mail spoofing?

A. Cryptographic signature
B. Uniform Resource Locator (URL) filtering
C. Spam filtering
D. Reverse Domain Name Service (DNS) lookup

**Correct Answer:** A
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 51**
In a High Availability (HA) environment, what is the **PRIMARY** goal of working with a virtual router address as the gateway to a network?

A. The second of two routers can periodically check in to make sure that the first router is operational.
B. The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.
C. The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.
D. The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

**Correct Answer:** C
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 52**
How does Encapsulating Security Payload (ESP) in transport mode affect in the Internet Protocol (IP)?

A. Authenticates the IP payload and selected portions of the IP header
B. Encrypts and optionally authenticates the complete IP packet
C. Encrypts and optionally authenticates the IP header, but not the IP payload
D. Encrypts and optionally authenticates the IP payload, but not the IP header

**Correct Answer:** D
**Section: Communication and Network Security**

**Explanation/Reference:**

**QUESTION 53**
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)

**Correct Answer:** D
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 54**
What protocol is often used between gateway hosts on the Internet?

A. Exterior Gateway Protocol (EGP)
B. Border Gateway Protocol (BGP)
C. Open Shortest Path First (OSPF)
D. Internet Control Message Protocol (ICMP)

**Correct Answer:** B
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 55**
“Stateful” differs from “Static” packet filtering firewalls by being aware of which of the following?

A. Difference between a new and an established connection
B. Originating network location
C. Difference between a malicious and a benign packet payload

D. Originating application session

**Correct Answer:** A
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 56**
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

**Correct Answer:** D
**Section: Communication and Network Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 57**
A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

A. Trusted third-party certification
B. Lightweight Directory Access Protocol (LDAP)
C. Security Assertion Markup language (SAML)
D. Cross-certification

**Correct Answer:** C
**Section: Identity and Access Management (IAM)**

**Explanation/Reference:**
Reference: https://www.netiq.com/documentation/access-manager-43/applications-configuration-guide/data/b1ka6lkd.html

**QUESTION 58**
Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

A. Derived credential
B. Temporary security credential
C. Mobile device credentialing service
D. Digest authentication

**Correct Answer:** A
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 59**
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

A. Limit access to predefined queries
B. Segregate the database into a small number of partitions each with a separate security level
C. Implement Role Based Access Control (RBAC)
D. Reduce the number of people who have access to the system for statistical purposes

**Correct Answer:** C
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 60**
What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

A. Audit logs
B. Role-Based Access Control (RBAC)
C. Two-factor authentication
D. Application of least privilege

**Correct Answer:** B
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 61**
Which of the following is the **BEST** metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

A. Application connection successes resulting in data leakage
B. Administrative costs for restoring systems after connection failure
C. Employee system timeouts from implementing wrong limits
D. Help desk costs required to support password reset requests

**Correct Answer:** D
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 62**
In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

A. Connect the device to another network jack
B. Apply remediation's according to security requirements
C. Apply Operating System (OS) patches
D. Change the Message Authentication Code (MAC) address of the network interface

**Correct Answer:** B

**Section: Identity and Access Management (IAM)**
**Explanation/Reference:**

**QUESTION 63**
What is the second step in the identity and access provisioning lifecycle?

A. Provisioning
B. Review
C. Approval
D. Revocation

**Correct Answer:** B
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 64**
Which of the following MUST be scalable to address security concerns raised by the integration of third-party identity services?

A. Mandatory Access Controls (MAC)
B. Enterprise security architecture
C. Enterprise security procedures
D. Role Based Access Controls (RBAC)

**Correct Answer:** D
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 65**
Which of the following is a common feature of an Identity as a Service (IDaaS) solution?

A. Single Sign-On (SSO) authentication support

B. Privileged user authentication support
C. Password reset service support

D. Terminal Access Controller Access Control System (TACACS) authentication support

**Correct Answer:** A
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 66**
An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

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

**Correct Answer:** A
**Section: Identity and Access Management (IAM)**
**Explanation**

**Explanation/Reference:**

**QUESTION 67**
Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

A. Change management processes
B. User administration procedures
C. Operating System (OS) baselines
D. System backup documentation

**Correct Answer:** A
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 68**
In which of the following programs is it MOST important to include the collection of security process data?

A. Quarterly access reviews
B. Security continuous monitoring
C. Business continuity testing
D. Annual security training

**Correct Answer:** A
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 69**
A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user's access to data files?

A. Host VM monitor audit logs
B. Guest OS access controls
C. Host VM access controls
D. Guest OS audit logs

**Correct Answer:** A
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 70**
Which type of test would an organization perform in order to locate and target exploitable defects?

A. Penetration
B. System
C. Performance
D. Vulnerability

**Correct Answer:** A
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 71**
What is the **MAIN** reason for testing a Disaster Recovery Plan (DRP)?

A. To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
B. To validate backup sites' effectiveness
C. To find out what does not work and fix it
D. To create a high level DRP awareness among Information Technology (IT) staff

**Correct Answer:** B
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 72**
When designing a vulnerability test, which one of the following is likely to give the **BEST** indication of what components currently operate on the network?

A. Ping testing
B. Mapping tools
C. Asset register
D. Topology diagrams

**Correct Answer:** B
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 73**

As part of an application penetration testing process, session hijacking can **BEST** be achieved by which of the following?

A. Known-plaintext attack
B. Denial of Service (DoS)
C. Cookie manipulation
D. Structured Query Language (SQL) injection

**Correct Answer:** D
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 74**
What are the steps of a risk assessment?

A. identification, analysis, evaluation
B. analysis, evaluation, mitigation
C. classification, identification, risk management
D. identification, evaluation, mitigation

**Correct Answer:** A
**Section: Security Assessment and Testing**
**Explanation**

**Explanation/Reference:**

**QUESTION 75**
An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

A. Absence of a Business Intelligence (BI) solution
B. Inadequate cost modeling
C. Improper deployment of the Service-Oriented Architecture (SOA)
D. Insufficient Service Level Agreement (SLA)

**Correct Answer:** D
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 76**
What is the PRIMARY reason for implementing change management?

A. Certify and approve releases to the environment
B. Provide version rollbacks for system changes
C. Ensure that all applications are approved
D. Ensure accountability for changes to the environment

**Correct Answer:** D
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 77**
Which of the following is a PRIMARY advantage of using a third-party identity service?

A. Consolidation of multiple providers
B. Directory synchronization
C. Web based logon
D. Automated account management

**Correct Answer:** D
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 78**

With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

A. Continuously without exception for all security controls
B. Before and after each change of the control
C. At a rate concurrent with the volatility of the security control
D. Only during system implementation and decommissioning

**Correct Answer:** B
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 79**
What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

A. Take the computer to a forensic lab
B. Make a copy of the hard drive
C. Start documenting
D. Turn off the computer

**Correct Answer:** C
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 80**
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

A. Disable all unnecessary services
B. Ensure chain of custody
C. Prepare another backup of the system
D. Isolate the system from the network

**Correct Answer:** D

**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 81**
A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

A. Guaranteed recovery of all business functions
B. Minimization of the need decision making during a crisis
C. Insurance against litigation following a disaster
D. Protection from loss of organization resources

**Correct Answer:** D
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 82**
Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

A. Hardware and software compatibility issues
B. Applications' critically and downtime tolerance
C. Budget constraints and requirements
D. Cost/benefit analysis and business objectives

**Correct Answer:** D
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**
Reference: http://www.pearsonitcertification.com/articles/article.aspx?p=1329710&seqNum=3

**QUESTION 83**
Which of the following is the FIRST step in the incident response process?

A. Determine the cause of the incident

B. Disconnect the system involved from the network
C. Isolate and contain the system involved
D. Investigate all symptoms to confirm the incident

**Correct Answer:** D
**Section: Security Operations Explanation**

**Explanation/Reference:**

**QUESTION 84**
A continuous information security monitoring program can BEST reduce risk through which of the following?

A. Collecting security events and correlating them to identify anomalies
B. Facilitating system-wide visibility into the activities of critical user accounts
C. Encompassing people, process, and technology
D. Logging both scheduled and unscheduled system changes

**Correct Answer:** B
**Section: Security Operations Explanation**

**Explanation/Reference:**

**QUESTION 85**
It is **MOST** important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

A. Negotiate schedule with the Information Technology (IT) operation's team
B. Log vulnerability summary reports to a secured server
C. Enable scanning during off-peak hours
D. Establish access for Information Technology (IT) management

**Correct Answer:** A
**Section: Security Operations**
**Explanation/Reference:**

**QUESTION 86**
A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established.

What MUST be considered or evaluated before performing the next step?

A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened
C. Removing the server from the network may prevent catching the intruder
D. Copying the contents of the hard drive to another storage device may damage the evidence

**Correct Answer:** C
**Section: Security Operations Explanation**

**Explanation/Reference:**

**QUESTION 87**
Which of the following is the **MOST** efficient mechanism to account for all staff during a speedy non-emergency evacuation from a large security facility?

A. Large mantrap where groups of individuals leaving are identified using facial recognition technology
B. Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exit door
C. Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list
D. Card-activated turnstile where individuals are validated upon exit

**Correct Answer:** B
**Section: Security Operations Explanation**

**Explanation/Reference:**

**QUESTION 88**
What does electronic vaulting accomplish?
A. It protects critical files.
B. It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems
C. It stripes all database records
D. It automates the Disaster Recovery Process (DRP)

**Correct Answer:** A
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 89**
An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

A. Perform a compliance review
B. Perform a penetration test
C. Train the technical staff
D. Survey the technical staff

**Correct Answer:** B
**Section: Security Operations**
**Explanation**

**Explanation/Reference:**

**QUESTION 90**
When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

A. After the system preliminary design has been developed and the data security categorization has been performed
B. After the vulnerability analysis has been performed and before the system detailed design begins
C. After the system preliminary design has been developed and before the data security categorization begins
D. After the business functional analysis and the data security categorization have been performed

**Correct Answer:** C
**Section: Software Development Security**
**Explanation/Reference:**

**QUESTION 91**
Which of the following is the BEST method to prevent malware from being introduced into a production environment?

A. Purchase software from a limited list of retailers
B. Verify the hash key or certificate key of all updates
C. Do not permit programs, patches, or updates from the Internet
D. Test all new software in a segregated environment

**Correct Answer:** D
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 92**
The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

A. System acquisition and development
B. System operations and maintenance
C. System initiation
D. System implementation

**Correct Answer:** A
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**
Reference https://online.concordia.edu/computer-science/system-development-life-cycle-phases/

**QUESTION 93**
What is the BEST approach to addressing security issues in legacy web applications?

A. Debug the security issues
B. Migrate to newer, supported applications where possible
C. Conduct a security assessment
D. Protect the legacy application with a web application firewall

**Correct Answer:** D

**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 94**
Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

A. Check arguments in function calls
B. Test for the security patch level of the environment
C. Include logging functions
D. Digitally sign each application module

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 95**
An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following **BEST** describes what has occurred?

A. Denial of Service (DoS) attack
B. Address Resolution Protocol (ARP) spoof
C. Buffer overflow
D. Ping flood attack

**Correct Answer:** A
**Section: Software Development Security**
**Explanation/Reference:**

**QUESTION 96**
In configuration management, what baseline configuration information **MUST** be maintained for each computer system?

A. Operating system and version, patch level, applications running, and versions.
B. List of system changes, test reports, and change approvals

C. Last vulnerability assessment report and initial risk assessment report
D. Date of last update, test report, and accreditation certificate

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 97**
Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

A. Notification tool
B. Message queuing tool
C. Security token tool
D. Synchronization tool

**Correct Answer:** C
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 98**
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

**Correct Answer:** B
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 99**
An application developer is deciding on the amount of idle session time that the application allows before a timeout. The **BEST** reason for determining the session timeout requirement is

A. organization policy.
B. industry best practices.
C. industry laws and regulations.
D. management feedback.

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 100**
During the Security Assessment and Authorization process, what is the **PRIMARY** purpose for conducting a hardware and software inventory?

A. Calculate the value of assets being accredited.
B. Create a list to include in the Security Assessment and Authorization package.
C. Identify obsolete hardware and software.
D. Define the boundaries of the information system.

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**
**QUESTION 101**
The goal of a Business Impact Analysis (BIA) is to determine which of the following?

A. Cost effectiveness of business recovery
B. Cost effectiveness of installing software security patches
C. Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
D. Which security measures should be implemented

**Correct Answer:** C
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 102**
How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

A. Examines log messages or other indications on the system.
B. Monitors alarms sent to the system administrator
C. Matches traffic patterns to virus signature files
D. Examines the Access Control List (ACL)

**Correct Answer:** C
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 103**
From a cryptographic perspective, the service of non-repudiation includes which of the following features?

A. Validity of digital certificates
B. Validity of the authorization rules
C. Proof of authenticity of the message
D. Proof of integrity of the message

**Correct Answer:** C
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 104**
Which of the following **BEST** represents the concept of least privilege? A. Access to an object is denied unless access is specifically

allowed.

https://vceplus.com/

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).

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 105**
Which of the following is an advantage of on-premise Credential Management Systems?

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

**Correct Answer:** B
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 106**
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.

**Correct Answer:** D
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 107**
Which of the following is the **PRIMARY** benefit of a formalized information classification program?

A. It minimized system logging requirements.
B. It supports risk assessment.
C. It reduces asset vulnerabilities.
D. It drives audit processes.

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 108**
Which of the following is the **BEST** method to reduce the effectiveness of phishing attacks?

A. User awareness
B. Two-factor authentication
C. Anti-phishing software
D. Periodic vulnerability scan

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 109**
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.

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 110**
When writing security assessment procedures, what is the **MAIN** purpose of the test outputs and reports?

A. To force the software to fail and document the process
B. To find areas of compromise in confidentiality and integrity
C. To allow for objective pass or fail decisions
D. To identify malware or hidden code within the test results

**Correct Answer:** C
**Section: Software Development Security Explanation**

**Explanation/Reference:**
**QUESTION 111**
A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the **MOST** suitable approach that the administrator should take?

A. Administrator should request data owner approval to the user access
B. Administrator should request manager approval for the user access

C. Administrator should directly grant the access to the non-sensitive files
D. Administrator should assess the user access need and either grant or deny the access

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 112**
How should an organization determine the priority of its remediation efforts after a vulnerability assessment has been conducted?

A. Use an impact-based approach.
B. Use a risk-based approach.
C. Use a criticality-based approach.
D. Use a threat-based approach.

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 113**
A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

A. Transport
B. Data link
C. Network
D. Application

**Correct Answer:** D
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 114**
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)

**Correct Answer:** D
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 115**
A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the **BEST** course of action?

A. Ignore the request and do not perform the change.
B. Perform the change as requested, and rely on the next audit to detect and report the situation.
C. Perform the change, but create a change ticket regardless to ensure there is complete traceability.
D. Inform the audit committee or internal audit directly using the corporate whistleblower process.

**Correct Answer:** D
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**
**QUESTION 116**
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

A. Tactical, strategic, and financial
B. Management, operational, and technical
C. Documentation, observation, and manual
D. Standards, policies, and procedures

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 117**
Which of the following BEST describes a chosen plaintext attack?

A. The cryptanalyst can generate ciphertext from arbitrary text.
B. The cryptanalyst examines the communication being sent back and forth.
C. The cryptanalyst can choose the key and algorithm to mount the attack.
D. The cryptanalyst is presented with the ciphertext from which the original message is determined.

**Correct Answer:** A
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 118**
For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

A. Alert data
B. User data
C. Content data
D. Statistical data

**Correct Answer:**
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**
D

**QUESTION 119**
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

**Correct Answer:** A
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 120**
What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

A. Information security practitioner
B. Information librarian
C. Computer operator
D. Network administrator

**Correct Answer:** B
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 121**

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.

**Correct Answer:** D
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 122**

Which of the following countermeasures is the **MOST** effective in defending against a social engineering attack?

A. Mandating security policy acceptance
B. Changing individual behavior
C. Evaluating security awareness training
D. Filtering malicious e-mail content

**Correct Answer:** C
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 123**

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

B

**Correct Answer:**
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**
**QUESTION 124**
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

**Correct Answer:** A
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 125**
Which of the following is considered a secure coding practice?

A. Use concurrent access for shared variables and resources
B. Use checksums to verify the integrity of libraries
C. Use new code for common tasks
D. Use dynamic execution functions to pass user supplied data

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 126**
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.

**Correct Answer:** D
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 127**
Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

A. Acoustic sensor
B. Motion sensor
C. Shock sensor
D. Photoelectric sensor

**Correct Answer:** C
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**

**QUESTION 128**
Which of the following is the **MOST** effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

B

**Correct Answer:**
**Section: Software Development Security**
**Explanation**

**Explanation/Reference:**
**QUESTION 129**
Which one of the following considerations has the **LEAST** impact when considering transmission security?

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

**Correct Answer:** C
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 130**
The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

A. System acquisition and development
B. System operations and maintenance
C. System initiation
D. System implementation

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 131**
Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?
A. Code quality, security, and origin
B. Architecture, hardware, and firmware
C. Data quality, provenance, and scaling
D. Distributed, agile, and bench testing

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 132**
What is the **PRIMARY** role of a scrum master in agile development?

A. To choose the primary development language
B. To choose the integrated development environment
C. To match the software requirements to the delivery plan
D. To project manage the software delivery

**Correct Answer:** D
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 133**
What capability would typically be included in a commercially available software package designed for access control?

A. Password encryption
B. File encryption
C. Source library control
D. File authentication

**Correct Answer:** A
**Section: Software Development Security**

**Explanation**

**Explanation/Reference:**

**QUESTION 134**
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

**Correct Answer:** B
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 135**
When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?

A. Implementation
B. Initiation
C. Review
D. Development

**Correct Answer:** A
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 136**
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

**Correct Answer:** C
**Section: Software Development Security Explanation**

**Explanation/Reference:**

**QUESTION 137**
Which of the following is the **MOST** important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

A. The likelihood and impact of a vulnerability
B. Application interface entry and endpoints
C. Countermeasures and mitigations for vulnerabilities
D. A data flow diagram for the application and attack surface analysis

**Correct Answer:** D
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 138**
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

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 139**
Which of the following is the **MOST** important activity an organization performs to ensure that security is part of the overall organization culture?

A. Perform formal reviews of security incidents.
B. Work with senior management to meet business goals.
C. Ensure security policies are issued to all employees.
D. Manage a program of security audits.

**Correct Answer:** A
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

**QUESTION 140**
What is the **MOST** common component of a vulnerability management framework?

A. Risk analysis
B. Patch management
C. Threat analysis
D. Backup management

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://www.helpnetsecurity.com/2016/10/11/effective-vulnerability-management-process/

**QUESTION 141**
What determines the level of security of a combination lock?
A. Complexity of combination required to open the lock
B. Amount of time it takes to brute force the combination
C. The number of barrels associated with the internal mechanism
D. The hardness score of the metal lock material

**Correct Answer:** A

**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**
Reference: https://books.google.com.pk/books?id=RbihG-YALUkC&pg=PA976&lpg=PA976&dq=CISSP+determines+the+level+of+security+of+a+combination+lock&source=bl&ots=ld6arg_Pl9&sig=ACfU3U0kh_Trrg6mQ65NmAP5PnUCIPmD0Q&hl=en&sa=X&ved=2ahUKEwjg69zN4KnpAhUJmRoKHR01B_MQ6AEwDHo ECBUQAQ#v=onepage&q=combination%20lock&f=false

**QUESTION 142**
An organization that has achieved a Capability Maturity Model Integration (CMMI) level of 4 has done which of the following?

A. Achieved optimized process performance
B. Achieved predictable process performance
C. Addressed the causes of common process variance
D. Addressed continuous innovative process improvement

**Correct Answer:** A
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**
Reference: https://www.sciencedirect.com/topics/computer-science/capability-maturity-model-integration

**QUESTION 143**
Which of the following is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services?

A. The acquiring organization
B. The service provider
C. The risk executive (function)
D. The IT manager

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 144**
Which of the following is the **PRIMARY** reason a sniffer operating on a network is collecting packets only from its own host?

A. An Intrusion Detection System (IDS) has dropped the packets.
B. The network is connected using switches.
C. The network is connected using hubs.
D. The network's firewall does not allow sniffing.

**Correct Answer:** A
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 145**
Which of the following is mobile device remote fingerprinting?

A. Installing an application to retrieve common characteristics of the device
B. Storing information about a remote device in a cookie file
C. Identifying a device based on common characteristics shared by all devices of a certain type
D. Retrieving the serial number of the mobile device

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 146**
Which of the following open source software issues pose the **MOST** risk to an application?
A. The software is beyond end of life and the vendor is out of business.
B. The software is not used or popular in the development community.
C. The software has multiple Common Vulnerabilities and Exposures (CVE) and only some are remediated.
D. The software has multiple Common Vulnerabilities and Exposures (CVE) but the CVEs are classified as low risks.

**Correct Answer:** D
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**

**QUESTION 147**
Which of the following is the **PRIMARY** mechanism used to limit the range of objects available to a given subject within different execution domains?

A. Process isolation
B. Data hiding and abstraction
C. Use of discrete layering and Application Programming Interfaces (API)
D. Virtual Private Network (VPN)

**Correct Answer:** C
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**
Reference: https://books.google.com.pk/books?id=LnjxBwAAQBAJ&pg=PT504&lpg=PT504&dq=CISSP+mechanism+used+to+limit+the+range+of+objects+available+to+a+given+subject+within+different+execution+domains&source=bl&ots=V-LJY4mkZy&sig=ACfU3U1adsKRObtT_l3tYTCLfHjS6gvLtg&hl=en&sa=X&ved=2ahUKEwi_jIPw16npAhWsxoUKHVoSA4AQ6AEwAHoECBMQAQ#v=onepage&q=CI SSP%20mechanism%20used%20to%20limit%20the%20range%20of%20objects%20available%20to%20a%20given%20subject%20within%20different%20execution%20domains&f=false

**QUESTION 148**
Once the types of information have been identified, who should an information security practitioner work with to ensure that the information is properly categorized?

A. Information Owner (IO)
B. System Administrator
C. Business Continuity (BC) Manager
D. Chief Information Officer (CIO)

**Correct Answer:** A
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 149**
What should be the **FIRST** action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

A. Isolate and contain the intrusion.
B. Notify system and application owners.
C. Apply patches to the Operating Systems (OS).
D. Document and verify the intrusion.

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://securityintelligence.com/dont-dwell-on-it-how-to-detect-a-breach-on-your-network-more-efficiently/

**QUESTION 150**
Which of the following needs to be taken into account when assessing vulnerability?

A. Risk identification and validation
B. Threat mapping
C. Risk acceptance criteria
D. Safeguard selection

**Correct Answer:** A
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA478&lpg=PA478&dq=CISSP+taken+into+account+when+assessing+vulnerability&source=bl&ots=riGvVpNN7I&sig=ACfU3U1isazG0OJlZdAAy91LvAW_rbXdAQ&hl=en&sa=X&ved=2ahUKEwj6p9vg4qnpAhUNxYUKHdODDZ4Q6AE wDHoECBMQAQ#v=onepage&q=CISSP%20taken%20into%20account%20when%20assessing%20vulnerability&f=false

**QUESTION 151**
Which of the following is **MOST** effective in detecting information hiding in Transmission Control Protocol/Internet Protocol (TCP/IP) traffic?

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

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 152**
An application team is running tests to ensure that user entry fields will not accept invalid input of any length. What type of negative testing is this an example of?

A. Reasonable data
B. Population of required fields
C. Allowed number of characters
D. Session testing

**Correct Answer:** C
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**
Reference: https://www.softwaretestinghelp.com/what-is-negative-testing/

**QUESTION 153**
An Internet software application requires authentication before a user is permitted to utilize the resource. Which testing scenario **BEST** validates the functionality of the application?

A. Reasonable data testing
B. Input validation testing
C. Web session testing
D. Allowed data bounds and limits testing

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 154**
A security architect is responsible for the protection of a new home banking system. Which of the following solutions can **BEST** improve the confidentiality and integrity of this external system?

A. Intrusion Prevention System (IPS)
B. Denial of Service (DoS) protection solution

C. One-time Password (OTP) token
D. Web Application Firewall (WAF)

**Correct Answer:** A
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**

**QUESTION 155**
What principle requires that changes to the plaintext affect many parts of the ciphertext?

A. Encapsulation
B. Permutation
C. Diffusion
D. Obfuscation

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Explanation:
Diffusion, on the other hand, means that a single plaintext bit has influence over several of the ciphertext bits. Changing a plaintext value should change many ciphertext values, not just one. In fact, in a strong block cipher, if one plaintext bit is changed, it will change every ciphertext bit with the probability of 50 percent. This means that if one plaintext bit changes, then about half of the ciphertext bits will change.

**QUESTION 156**
Which of the following **BEST** describes how access to a system is granted to federated user accounts?

A. With the federation assurance level
B. Based on defined criteria by the Relying Party (RP)
C. Based on defined criteria by the Identity Provider (IdP)
D. With the identity assurance level

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://resources.infosecinstitute.com/cissp-domain-5-refresh-identity-and-access-management/

**QUESTION 157**
Which of the following is the primary advantage of segmenting Virtual Machines (VM) using physical networks?

A. Simplicity of network configuration and network monitoring
B. Removes the need for decentralized management solutions
C. Removes the need for dedicated virtual security controls
D. Simplicity of network configuration and network redundancy

**Correct Answer:** A
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 158**
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

**Correct Answer:** B
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**
Reference: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/vulnerability-and-patch-management/#gref

**QUESTION 159**
A development operations team would like to start building new applications delegating the cybersecurity responsibility as much as possible to the service provider. Which of the following environments **BEST** fits their need?

A. Cloud Virtual Machines (VM)
B. Cloud application container within a Virtual Machine (VM)

C. On premises Virtual Machine (VM)
D. Self-hosted Virtual Machine (VM)

**Correct Answer:** A
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 160**
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)

**Correct Answer:** D
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://en.wikipedia.org/wiki/Attribute-based_access_control

**QUESTION 161**
Why is planning the **MOST** critical phase of a Role Based Access Control (RBAC) implementation?

A. The criteria for measuring risk is defined.
B. User populations to be assigned to each role is determined.
C. Role mining to define common access patterns is performed.
D. The foundational criteria are defined.

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 162**

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

**Correct Answer:** C
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**

**QUESTION 163**
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

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 164**
Compared with hardware cryptography, software cryptography is generally

A. less expensive and slower.
B. more expensive and faster.
C. more expensive and slower.
D. less expensive and faster.

**Correct Answer:** A
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**
Reference: https://www.ontrack.com/uk/blog/making-data-simple/hardware-encryption-vs-software-encryption-the-simple-guide/

**QUESTION 165**
A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

A. No, because the encryption solution is internal to the cloud provider.
B. Yes, because the cloud provider meets all regulations requirements.
C. Yes, because the cloud provider is GDPR compliant.
D. No, because the cloud provider is not certified to host government data.

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**
**QUESTION 166**
What is the **MAIN** purpose for writing planned procedures in the design of Business Continuity Plans (BCP)?

A. Establish lines of responsibility.
B. Minimize the risk of failure.
C. Accelerate the recovery process.
D. Eliminate unnecessary decision making.

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 167**
Why might a network administrator choose distributed virtual switches instead of stand-alone switches for network segmentation?

A. To standardize on a single vendor
B. To ensure isolation of management traffic
C. To maximize data plane efficiency

D. To reduce the risk of configuration errors

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 168**
Which of the following is the **BEST** reason to apply patches manually instead of automated patch management?

A. The cost required to install patches will be reduced.
B. The time during which systems will remain vulnerable to an exploit will be decreased.
C. The target systems reside within isolated networks.
D. The ability to cover large geographic areas is increased.

**Correct Answer:** C
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**

**QUESTION 169**
When should the software Quality Assurance (QA) team feel confident that testing is complete?

A. When release criteria are met
B. When the time allocated for testing the software is met
C. When senior management approves the test results
D. When the software has zero security vulnerabilities

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 170**

A system administration office desires to implement the following rules:

▪ An administrator that is designated as a skill level 3, with 5 years of experience, is allowed to perform system backups, upgrades, and local administration. ▪ An administrator that is designated as a skill level 5, with 10 years of experience, is permitted to perform all actions related to system administration.

Which of the following access control methods **MUST** be implemented to achieve this goal?

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

**Correct Answer:** B
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**

**QUESTION 171**
Which of the following **MUST** a security policy include to be effective within an organization?

A. A list of all standards that apply to the policy
B. Owner information and date of last revision
C. Disciplinary measures for non-compliance
D. Strong statements that clearly define the problem

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 172**
What is the **MOST** efficient way to verify the integrity of database backups?

A. Test restores on a regular basis.
B. Restore every file in the system to check its health.

C. Use checksum as part of the backup operation to make sure that no corruption has occurred.
D. Run DBCC CHECKDB on a regular basis to check the logical and physical integrity of the database objects.

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 173**
What information will **BEST** assist security and financial analysts in determining if a security control is cost effective to mitigate a vulnerability?

A. Annualized Loss Expectancy (ALE) and the cost of the control
B. Single Loss Expectancy (SLE) and the cost of the control
C. Annual Rate of Occurrence (ARO) and the cost of the control
D. Exposure Factor (EF) and the cost of the control

**Correct Answer:** D
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 174**
Which of the following are the **FIRST** two steps to securing employees from threats involving workplace violence and acts of terrorism?

A. Physical barriers impeding unauthorized access and security guards at each entrance
B. Physical barriers and the ability to identify people as they enter the workplace
C. Security guards and metal detectors posted at each entrance
D. Metal detectors and the ability to identify people as they enter the workplace

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 175**

How can an attacker exploit a stack overflow to execute arbitrary code?

A. Modify a function’s return address.
B. Move the stack pointerC. Substitute elements in the stack.
D. Alter the address of the stack.

**Correct Answer:** A
**Section: Mixed questions Explanation**

**Explanation/Reference:**
**QUESTION 176**
A security team member was selected as a member of a Change Control Board (CCB) for an organization. Which of the following is one of their responsibilities?

A. Approving or disapproving the change
B. Determining the impact of the change
C. Carrying out the requested change
D. Logging the change

**Correct Answer:** B
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**

**QUESTION 177**
Which action is **MOST** effective for controlling risk and minimizing maintenance costs in the software supply chain?

A. Selecting redundant suppliers
B. Selecting suppliers based on business requirements
C. Selecting fewer, more reliable suppliers
D. Selecting software suppliers with the fewest known vulnerabilities

**Correct Answer:** D
**Section: Mixed questions**
**Explanation**

**Explanation/Reference:**

**QUESTION 178**
A group of organizations follows the same access standards and practices. One manages the verification and due diligence processes for the others. For a user to access a resource from one of the organizations, a check is made to see if that user has been certified. Which Federated Identity Management (FIM) process is this an example of?

A. One-time authentication
B. Web based access management
C. Cross-certification model
D. Bridge model

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 179**
The process of “salting” a password is designed to increase the difficulty of cracking which of the following?

A. Specific password
B. Password hash function
C. Password algorithm
D. Maximum password length

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

**QUESTION 180**
Which of the following benefits does Role Based Access Control (RBAC) provide for the access review process?

A. Lowers the amount of access requests after review
B. Gives more control into the revocation phase
C. Gives more fine-grained access analysis to accesses
D. Lowers the number of items to be reviewed

**Correct Answer:** C
**Section: Mixed questions Explanation**

**Explanation/Reference:**
**QUESTION 181**
Which of the following is the **BEST** type of authentication and encryption for a Secure Shell (SSH) implementation when network traffic traverses between a host and an infrastructure device?

A. Lightweight Directory Access Protocol (LDAP)
B. Public-key cryptography
C. Remote Authentication Dial-In User Service (RADIUS)
D. Private-key cryptography

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://books.google.com.pk/books?id=4K7LCgAAQBAJ&pg=PA284&lpg=PA284&dq=type+of+authentication+and+encryption+for+a+Secure+Shell+(SSH)+implementation+when+network+traffic+traverses+between+a+host+and+an+infrastructure+device&source=bl&ots=YEMNN8nfuN&sig=ACfU3U2QMbLySWQ_0Vs-GjsSJmaHZ_O9Iw&hl=en&sa=X&ved=2ahUKEwjDobCajqrpAhWMHRQKHW2FC4gQ6AEwAHoECBQQAQ#v=onepage&q=type%20of%20authentication%20and%20encryption%20for%20a%20Secure%20Shell%20(SSH)%20implementation%20when%20network%20traffic%20traverses%20between%20a%20host%20and%20an%20infrastructure%20device&f=false

**QUESTION 182**
Which of the following is the **FIRST** thing to consider when reviewing Information Technology (IT) internal controls?

A. The risk culture of the organization
B. The impact of the control
C. The nature of the risk
D. The cost of the control

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 183**
Which layer of the Open System Interconnection (OSI) model is reliant on other layers and is concerned with the structure, interpretation and handling of information?

A. Presentation Layer
B. Session Layer
C. Application Layer
D. Transport Layer

**Correct Answer:** D
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 184**
Which concept might require users to use a second access token or to re-enter passwords to gain elevated access rights in the identity and access provisioning life cycle?

A. Time-based
B. Enrollment
C. Least privilegeD. Access review

**Correct Answer:** B
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 185**
Why are mobile devices sometimes difficult to investigate in a forensic examination?

A. There are no forensics tools available for examination.
B. They may contain cryptographic protection.
C. They have password-based security at logon.
D. They may have proprietary software installed to protect them.

**Correct Answer:** D
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 186**
Security categorization of a new system takes place during which phase of the Systems Development Life Cycle (SDLC)?

A. System implementation
B. System initiation
C. System operations and maintenanceD. System acquisition and development

**Correct Answer:** D
**Section: Mixed questions Explanation**

**Explanation/Reference:**

**QUESTION 187**
What is the motivation for use of the Online Certificate Status Protocol (OCSP)?

A. To return information on multiple certificates
B. To control access to Certificate Revocation List (CRL) requests
C. To provide timely up-to-date responses to certificate queries
D. To issue X.509v3 certificates more quickly

**Correct Answer:** D
**Section: Mixed questions Explanation**

**Explanation/Reference:**
Reference: https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

https://vceplus.com/