CISSP.premium.162q - DEMO

Number: CISSP
Passing Score: 800
Time Limit: 120 min

CISSP

Certified Information Systems Security Professional

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
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 actions will reduce risk to a laptop before traveling to a high risk area?

A. Examine the device for physical tampering
B. Implement more stringent baseline configurations
C. Purge or re-image the hard disk drive
D. Change access codes

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:

QUESTION 3 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 4
What is the MOST important consideration from a data security perspective when an organization plans to relocate?

A. Ensure the fire prevention and detection systems are sufficient to protect personnel
B. Review the architectural plans to determine how many emergency exits are present
C. Conduct a gap analysis of a new facilities against existing security requirements
D. Revise the Disaster Recovery and Business Continuity (DR/BC) plan

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:

QUESTION 5
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 6
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 7
Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

A. Install mantraps at the building entrances
B. Enclose the personnel entry area with polycarbonate plastic
C. Supply a duress alarm for personnel exposed to the public
D. Hire a guard to protect the public area

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:

QUESTION 8
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 9 Intellectual property rights are PRIMARY concerned with which of the following?

A. Owner's ability to realize financial gain
B. Owner's ability to maintain copyright
C. Right of the owner to enjoy their creation
D. Right of the owner to control delivery method

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:

QUESTION 10 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 11 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 12 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 securityD. 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 13
An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.

Which contract is BEST in offloading the task from the IT staff?

A. Platform as a Service (PaaS)
B. Identity as a Service (IDaaS)
C. Desktop as a Service (DaaS)
D. Software as a Service (SaaS)

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:

QUESTION 14 When implementing a data classification program, why is it important to avoid too much granularity?

A. The process will require too many resources
B. It will be difficult to apply to both hardware and software
C. It will be difficult to assign ownership to the data
D. The process will be perceived as having value

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Reference: http://www.ittoday.info/AIMS/DSM/82-02-55.pdf

QUESTION 15 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 16
Which of the following is an initial consideration when developing an information security management system?

A. Identify the contractual security obligations that apply to the organizations
B. Understand the value of the information assets
C. Identify the level of residual risk that is tolerable to management
D. Identify relevant legislative and regulatory compliance requirements

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 security service is served by the process of encryption plaintext with the sender's private key and decrypting cipher text with the sender's public key?

A. Confidentiality
B. Integrity
C. Identification
D. Availability

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:

QUESTION 19 Which of the following mobile code security models relies only on trust?

A. Code signing
B. Class authentication
C. Sandboxing
D. Type safety

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:
Reference: https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/t09.pdf (11)

QUESTION 20 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 21 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 22
Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

A. Common Vulnerabilities and Exposures (CVE)
B. Common Vulnerability Scoring System (CVSS)
C. Asset Reporting Format (ARF)
D. Open Vulnerability and Assessment Language (OVAL)

Correct Answer: B
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:

QUESTION 23
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 24 The use of private and public encryption keys is fundamental in the implementation of which of the following?

A. Diffie-Hellman algorithm
B. Secure Sockets Layer (SSL)
C. Advanced Encryption Standard (AES)
D. Message Digest 5 (MD5)

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:

QUESTION 25 What is the purpose of an Internet Protocol (IP) spoofing attack?

A. To send excessive amounts of data to a process, making it unpredictable
B. To intercept network traffic without authorization
C. To disguise the destination address from a target's IP filtering devices
D. To convince a system that it is communicating with a known entity

Correct Answer: D
Section: Communication and Network Security
QUESTION 26
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

Explanation

Explanation/Reference:

A. Link layer
B. Physical layer
C. Session layer
D. Application layer

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 27
In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

A. Transport layer
B. Application layer
C. Network layer
D. Session layer

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 28 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 29 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 30
An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

A. Implement packet filtering on the network firewalls
B. Install Host Based Intrusion Detection Systems (HIDS)
C. Require strong authentication for administrators
D. Implement logical network segmentation at the switches

Correct Answer: D
Section: Communication and Network Security
QUESTION 31
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

Explanation

Explanation/Reference:

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 32
Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

A. Intrusion Prevention Systems (IPS)
B. Intrusion Detection Systems (IDS)
C. Stateful firewalls
D. Network Behavior Analysis (NBA) tools

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 33
Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

A. WEP uses a small range Initialization Vector (IV)
B. WEP uses Message Digest 5 (MD5)
C. WEP uses Diffie-Hellman
D. WEP does not use any Initialization Vector (IV)

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Reference: http://www.dummies.com/programming/networking/understanding-wep-weaknesses/

QUESTION 34
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

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

QUESTION 35
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 36
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 37
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 38
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 39
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 40
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 41
Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

A. Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken
B. Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability
C. Management teams will understand the testing objectives and reputational risk to the organization
D. Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels

Correct Answer: D
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

QUESTION 42 Which of the following could cause a Denial of Service (DoS) against an authentication system?

A. Encryption of audit logs
B. No archiving of audit logs
C. Hashing of audit logs
D. Remote access audit logs

Correct Answer: D
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

QUESTION 43

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 44
Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

A. Walkthrough
B. Simulation
C. Parallel
D. White box

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Reference: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61029/Chapter-6-Business-ContinuityManagement_amends_04042012.pdf

QUESTION 45
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 46 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 47
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 48

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

Correct Answer:

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 49 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 50 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 51 When is a Business Continuity Plan (BCP) considered to be valid?

A. When it has been validated by the Business Continuity (BC) manager
B. When it has been validated by the board of directors
C. When it has been validated by all threat scenarios
D. When it has been validated by realistic exercises

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Reference: http://www.manchester.gov.uk/info/200039/emergencies/6174/business_continuity_planning/5

QUESTION 52 Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

A. Hardware and software compatibility issues
B. Applications' criticality 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 53 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 54
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 55
What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

A. Warm site
B. Hot site
C. Mirror site
D. Cold site

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

QUESTION 56
A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

A. Least privilege
B. Privilege escalation
C. Defense in depth
D. Privilege bracketing

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 57
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

A. Lack of software documentation
B. License agreements requiring release of modified code
C. Expiration of the license agreement
D. Costs associated with support of the software

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 58
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 beginsD. After the business functional analysis and the data security categorization have been performed

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 59
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 60
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 61 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 62
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 63
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

Explanation/Reference:

QUESTION 64 Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

A. dig
B. ipconfig
C. ifconfig
D. nbstat

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 65 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 66 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

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 67 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.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 68 When building a data classification scheme, which of the following is the **PRIMARY** concern?

A.

Explanation/Reference:

Purpose
Cost effectiveness

C. Availability
D. Authenticity

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 69 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 70 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

C

A.

B.

QUESTION 71 Backup information that is critical to the organization is identified through a

A. Vulnerability Assessment (VA).
B. Business Continuity Plan (BCP).
C. Business Impact Analysis (BIA).
D. data recovery analysis.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 72
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 73
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 organization policy.

Correct Answer:
Section: Software Development Security
Explanation

Explanation/Reference:

industry best practices.
C. industry laws and regulations.
D. management feedback.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 74 Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

A. clear-text attack.
B. known cipher attack.
C. frequency analysis.
D. stochastic assessment.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 75
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.

A

QUESTION 76
A.

B.

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.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 77
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.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 78 The goal of a Business Impact Analysis (BIA) is to determine which of the following?

Cost effectiveness of business recovery

Correct Answer:
Section: Software Development Security
Explanation

Explanation/Reference:

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 79
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a **PRIMARY** security concern?

A. Ownership
B. Confidentiality
C. Availability
D. Integrity

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 80
What does the Maximum Tolerable Downtime (MTD) determine?

A. The estimated period of time a business critical database can remain down before customers are affected.
B. The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning
C. The estimated period of time a business can remain interrupted beyond which it risks never recoveringD. The fixed length of time in a DR process before redundant systems are engaged

C

A.

Explanation/Reference:

QUESTION 81 What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

A. SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).
B. SSL and TLS provide nonrepudiation by default.
C. SSL and TLS do not provide security for most routed protocols.
D. SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 82 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 83 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 84 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).

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 85 Which of the following is an advantage of on-premise Credential Management Systems?

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

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
QUESTION 86
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. Topology diagrams

B. Mapping tools
C. Asset register
D. Ping testing

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 87 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 88 Which of the following **BEST** describes Recovery Time Objective (RTO)?

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

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 89 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 90 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 91 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 92 Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

A. Length of Initialization Vector (IV)
B. Protection against message replay
C. Detection of message tampering
D. Built-in provision to rotate keys

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 93 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 94 Which of the following is the **MAIN** reason for using configuration management?

A. To provide centralized administration
B. To reduce the number of changes
C. To reduce errors during upgrades
D. To provide consistency in security controls

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 95
Which of the following is **BEST** suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAML)
C. Internet Mail Access Protocol
D. Transport Layer Security (TLS)

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
QUESTION 96 Which of the following is **MOST** important when deploying digital certificates?

A. Validate compliance with X.509 digital certificate standards
B. Establish a certificate life cycle management framework
C. Use a third-party Certificate Authority (CA)
D. Use no less than 256-bit strength encryption when creating a certificate

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 97
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 98
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 99 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

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 100 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 101 Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Mandatory vacations

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 102 Although code using a specific program language may not be susceptible to a buffer overflow attack,

A. most calls to plug-in programs are susceptible.
B. most supporting application code is susceptible.
C. the graphical images used by the application could be susceptible.
D. the supporting virtual machine could be susceptible.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 103 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 104 Which of the following are effective countermeasures against passive network-layer attacks?

A. Federated security and authenticated access controls
B. Trusted software development and run time integrity controls
C. Encryption and security enabled applications
D. Enclave boundary protection and computing environment defense

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 105
What is the **MOST** important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

A. Management support
B. Consideration of organizational need
C. Technology used for delivery
D. Target audience

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 106
DRAG DROP
Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

Select and Place:

Access Control Model		Restrictions
Mandatory Access Control		End user cannot set controls
Discretionary Access Control (DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule based access control		Dynamically assigns roles to subjects based on criteria assigned by a custodian

Correct Answer:

Access Control Model		Restrictions
	Mandatory Access Control	End user cannot set controls
	Discretionary Access Control (DAC)	Subject has total control over objects
	Role Based Access Control (RBAC)	Dynamically assigns permissions to particular duties based on job function
	Rule based access control	Dynamically assigns roles to subjects based on criteria assigned by a custodian

Section: Software Development Security
Explanation
Explanation/Reference:

QUESTION 107
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 108 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

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 109
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 110
Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

A. VPN bandwidth
B. Simultaneous connection to other networks
C. Users with Internet Protocol (IP) addressing conflicts
D. Remote users with administrative rights

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 111 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

C.

Explanation/Reference:

QUESTION 112
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: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 113 Which of the following is the **PRIMARY** reason to perform regular vulnerability scanning of an organization network?

A. Provide vulnerability reports to management.
B. Validate vulnerability remediation activities.
C. Prevent attackers from discovering vulnerabilities.
D. Remediate known vulnerabilities.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 114 Which of the following would **BEST** describe the role directly responsible for data within an organization?

A. Data custodian Information owner Database administrator

D. Quality control

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 115 The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

A. Service Level Agreement (SLA)
B. Business Continuity Plan (BCP)
C. Business Impact Analysis (BIA)
D. Crisis management plan

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 116 The **PRIMARY** outcome of a certification process is that it provides documented

A. interconnected systems and their implemented security controls.
B. standards for security assessment, testing, and process evaluation.
C. system weakness for remediation.
D. security analyses needed to make a risk-based decision.

Correct Answer: D

B.

C.

Section: Software Development Security
Explanation

Explanation/Reference:
QUESTION 117
A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

A. Confidentiality
B. Integrity
C. Availability
D. Accessibility

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 118 A vulnerability in which of the following components would be **MOST** difficult to detect?

A. Kernel
B. Shared libraries
C. Hardware
D. System application

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 119 During which of the following processes is least privilege implemented for a user account?

A. Provision
Approve
Request
D. Review

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 120
Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

A. Property book
B. Chain of custody form
C. Search warrant return
D. Evidence tag

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 121 Which of the following is needed to securely distribute symmetric cryptographic keys?

A. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates
B. Officially approved and compliant key management technology and processes
C. An organizationally approved communication protection policy and key management plan
D. Hardware tokens that protect the user's private key.

Correct Answer: C

B.

C.

Section: Software Development Security
Explanation
Explanation/Reference:

QUESTION 122 Reciprocal backup site agreements are considered to be

A. a better alternative than the use of warm sites.
B. difficult to test for complex systems.
C. easy to implement for similar types of organizations.
D. easy to test and implement for complex systems.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 123 In which identity management process is the subject's identity established?

A. Trust
B. Provisioning
C. Authorization
D. Enrollment

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 124 In order to assure authenticity, which of the following are required?

A. Confidentiality and authentication
Confidentiality and integrity
Authentication and non-repudiation
D. Integrity and non-repudiation

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 125
At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

A. Transport Layer
B. Data-Link Layer
C. Network Layer
D. Application Layer

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 126
An organization regularly conducts its own penetration tests. Which of the following scenarios **MUST** be covered for the test to be effective?

A. Third-party vendor with access to the system
B. System administrator access compromised
C. Internal attacker with access to the system
D. Internal user accidentally accessing data

Correct Answer: C

B.

C.

Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 127
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 128 What is the difference between media marking and media labeling?

A. Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.
B. Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
C. Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
D. Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizationalpolicy.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 129
What balance **MUST** be considered when web application developers determine how informative application error messages should be constructed?
A. Risk versus benefit
B. Availability versus auditability
C. Confidentiality versus integrity

D. Performance versus user satisfaction

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 130 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 131 Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A. It must be known to both sender and receiver.
B. It can be transmitted in the clear as a random number.
C. It must be retained until the last block is transmitted.
D. It can be used to encrypt and decrypt information.

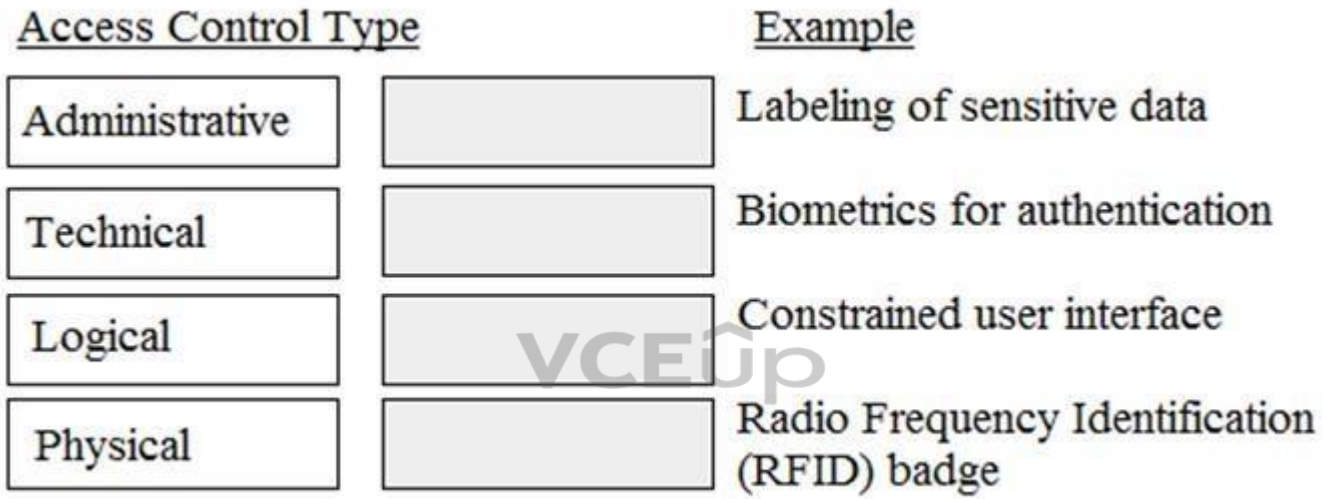
Correct Answer: B
Section: Software Development Security
Explanation
Explanation/Reference:

QUESTION 132
DRAG DROP

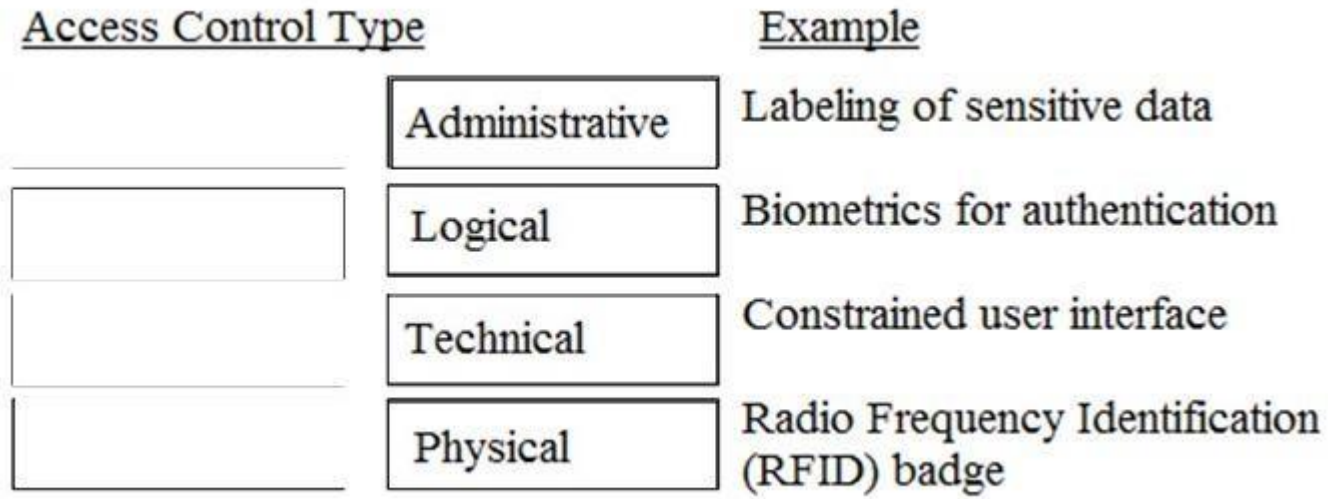
Match the access control type to the example of the control type.

Drag each access control type net to its corresponding example.

Select and Place:



Correct Answer:



Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 133
In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is **MAIN** purpose of the DMZ?

A. Reduced risk to internal systems.
B. Prepare the server for potential attacks.
C. Mitigate the risk associated with the exposed server.
D. Bypass the need for a firewall.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
QUESTION 134

Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

A. Addresses and protocols of network-based logs are analyzed.
B. Host-based system logging has files stored in multiple locations.
C. Properly handled network-based logs may be more reliable and valid.
D. Network-based systems cannot capture users logging into the console.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 135
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 136
Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

A. Transport and Session
B. Data-Link and Transport
C. Network and Session
D. Physical and Data-Link
Correct Answer: B

Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 137
Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

A. Reversal
B. Gray box
C. Blind
D. White box

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 138
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 139 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

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 140
Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

A. Temporal Key Integrity Protocol (TKIP)
B. Secure Hash Algorithm (SHA)
C. Secure Shell (SSH)
D. Transport Layer Security (TLS)

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 141
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 142 In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

A. systems integration.
B. risk management.
C. quality assurance.
D. change management.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 143 As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

A. Data classification policy
B. Software and hardware inventory
C. Remediation recommendations
D. Names of participants

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 144
The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

A. require an update of the Protection Profile (PP).
B. require recertification.
C. retain its current EAL rating.
D. reduce the product to EAL 3.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 145
Which of the following media sanitization techniques is **MOST** likely to be effective for an organization using public cloud services?

A. Low-level formatting
B. Secure-grade overwrite erasure
C. Cryptographic erasure
D. Drive degaussing

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 146 What type of wireless network attack **BEST** describes an Electromagnetic Pulse (EMP) attack?

A. Radio Frequency (RF) attack
B. Denial of Service (DoS) attack
C. Data modification attack
D. Application-layer attack

Correct Answer: B
Section: Software Development Security
Explanation

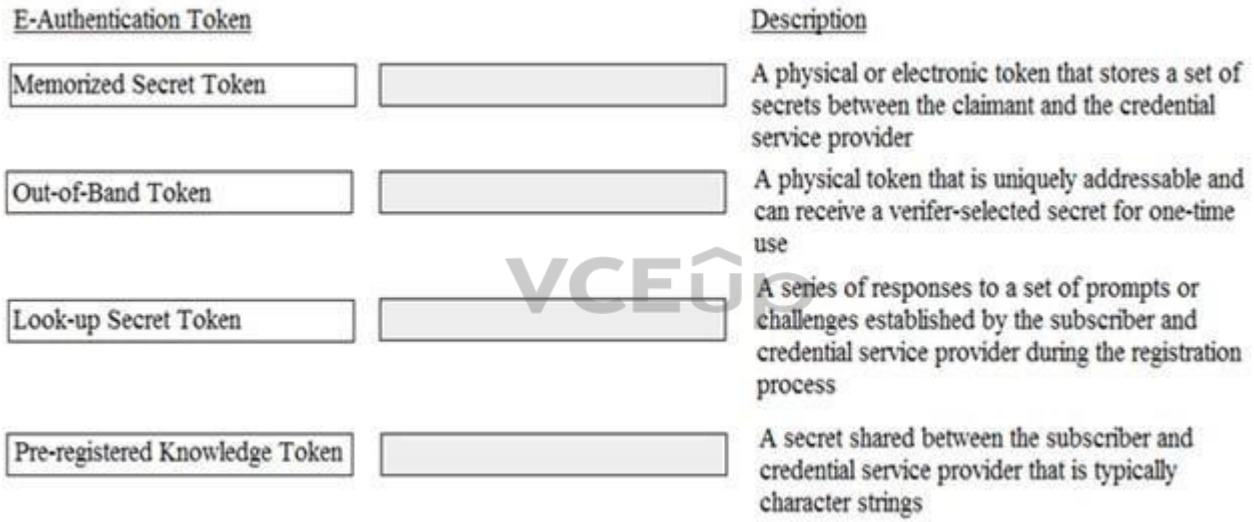
Explanation/Reference:

QUESTION 147
DRAG DROP

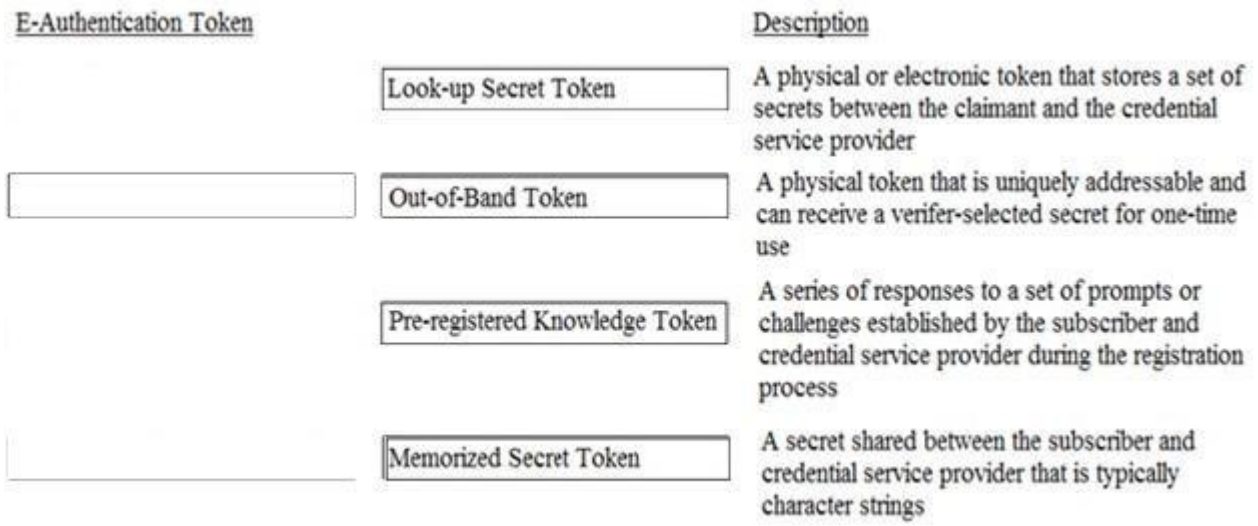
Match the types of e-authentication tokens to their description.

Drag each e-authentication token on the left to its corresponding description on the right.

Select and Place:



Correct Answer:



Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 148 Which of the following is a remote access protocol that uses a static authentication?

A. Point-to-Point Tunneling Protocol (PPTP)
B. Routing Information Protocol (RIP)
C. Password Authentication Protocol (PAP)
D. Challenge Handshake Authentication Protocol (CHAP)

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
QUESTION 149

Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

A. Logging and audit trail controls to enable forensic analysis
B. Security incident response lessons learned procedures
C. Security event alert triage done by analysts using a Security Information and Event Management (SIEM) systemD. Transactional controls focused on fraud prevention

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 150 Determining outage costs caused by a disaster can **BEST** be measured by the

A. cost of redundant systems and backups.
B. cost to recover from an outage.
C. overall long-term impact of the outage.
D. revenue lost during the outage.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 151 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 152
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 153 Who has the **PRIMARY** responsibility to ensure that security objectives are aligned with organization goals?

A. Senior management
B. Information security department
C. Audit committee
D. All users

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
QUESTION 154
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 155 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.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 156
Which of the following is the **MOST** important part of an awareness and training plan to prepare employees for emergency situations?

A. Having emergency contacts established for the general employee population to get information
B. Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
C. Designing business continuity and disaster recovery training programs for different audiences
D. Publishing a corporate business continuity and disaster recovery plan on the corporate website

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 157
What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

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

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 158 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 159
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 160
DRAG DROP

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

Select and Place:

Security Engineering Term		Definition
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.

Correct Answer:

Security Engineering Term		Definition
	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
	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 the 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.

Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 161 Which of the following is the **BEST** reason for the use of security metrics?

A. They ensure that the organization meets its security objectives.
B. They provide an appropriate framework for Information Technology (IT) governance.
C. They speed up the process of quantitative risk assessment.
D. They quantify the effectiveness of security processes.

Correct Answer: B
Section: Software Development Security

Explanation

Explanation/Reference:

QUESTION 162 Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A. Password requirements are simplified.
B. Risk associated with orphan accounts is reduced.
C. Segregation of duties is automatically enforced.
D. Data confidentiality is increased.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference: