ISC.CISSP.by.Antony.543q

Number: CISSP
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: CISSP
Exam Name: Certified Information Systems Security Professional

Exam A

QUESTION 1
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: C
Section:

QUESTION 2
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: D
Section:

QUESTION 3
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:

QUESTION 4
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: D

Section:

QUESTION 5
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:

QUESTION 6
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: C
Section:

QUESTION 7
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:

QUESTION 8
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: D

Section:

QUESTION 9

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: A

Section:

QUESTION 10

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:

QUESTION 11

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:

QUESTION 12

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: D

Section:

QUESTION 13

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:

QUESTION 14
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:

QUESTION 15
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:

QUESTION 16
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: B
Section:

QUESTION 17
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:

QUESTION 18
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

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

Correct Answer: D
Section:

QUESTION 19
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:

QUESTION 20
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:

QUESTION 21
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:

QUESTION 22
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:

QUESTION 23
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:

QUESTION 24
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:

QUESTION 25
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:

QUESTION 26
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:

QUESTION 27
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:

QUESTION 28
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:

QUESTION 29
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:

QUESTION 30
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:

QUESTION 31
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: B
Section:

QUESTION 32
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:

QUESTION 33
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:

QUESTION 34
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:

QUESTION 35
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:

QUESTION 36
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: C
Section:

QUESTION 37
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:

QUESTION 38
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:

QUESTION 39
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:

QUESTION 40
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:

QUESTION 41
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:

QUESTION 42
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:

QUESTION 43
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:

QUESTION 44
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:

QUESTION 45
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:

QUESTION 46
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:

QUESTION 47
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:

QUESTION 48
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:

QUESTION 49
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:

QUESTION 50
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: D
Section:

QUESTION 51
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:

QUESTION 52
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:
Explanation:
Reference https://online.concordiA.edu/computer-science/system-development-life-cycle-phases/

QUESTION 53
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:

QUESTION 54
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:

QUESTION 55
Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

A. Transparent Database Encryption (TDE)
B. Column level database encryption
C. Volume encryption

D. Data tokenization

Correct Answer: D
Section:

QUESTION 56
Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

A. An of how long the data subject's collected information will be retained for and how it will be eventually disposed.
B. An of who can be contacted at the organization collecting the information if corrections are required by the data subject.
C. An of the regulatory frameworks and compliance standards the information collecting organization adheres to.
D. An of all the technologies employed by the collecting organization in gathering information on the data subject.

Correct Answer: B
Section:

QUESTION 57
What is the MOST effective countermeasure to a malicious code attack against a mobile system?

A. Sandbox
B. Change control
C. Memory management
D. Public-Key Infrastructure (PKI)

Correct Answer: A
Section:

QUESTION 58
Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring
B. Security awareness training
C. Corporate policy and procedures
D. Strong file and directory permissions

Correct Answer: B
Section:

QUESTION 59
Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?

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

Correct Answer: A

Section:

QUESTION 60

Which of the following is an essential element of a privileged identity lifecycle management?

A. Regularly perform account re-validation and approval

B. Account provisioning based on multi-factor authentication

C. Frequently review performed activities and request justification

D. Account information to be provided by supervisor or line manager

Correct Answer: A

Section:

QUESTION 61

Which of the following is ensured when hashing files during chain of custody handling?

A. Availability

B. Accountability

C. Integrity

D. Non-repudiation

Correct Answer: C

Section:

QUESTION 62

Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

A. Cross Origin Resource Sharing (CORS)

B. WebSockets

C. Document Object Model (DOM) trees

D. Web Interface Definition Language (IDL)

Correct Answer: B

Section:

QUESTION 63

Which of the following statements is TRUE of black box testing?

A. Only the functional specifications are known to the test planner.

B. Only the source code and the design documents are known to the test planner.

C. Only the source code and functional specifications are known to the test planner.

D. Only the design documents and the functional specifications are known to the test planner.

Correct Answer: A

Section:

QUESTION 64

A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?

A. Encryption routines
B. Random number generator
C. Obfuscated code
D. Botnet command and control

Correct Answer: C
Section:

QUESTION 65
What security management control is MOST often broken by collusion?

A. Job rotation
B. Separation of duties
C. Least privilege model
D. Increased monitoring

Correct Answer: B
Section:

QUESTION 66
An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is
MOST likely occurring?

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

Correct Answer: A
Section:

QUESTION 67
An engineer in a software company has created a virus creation tool. The tool can generate thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled environment to test the company's next generation virus scanning software. Which would BEST describe the behavior of the engineer and why?

A. The behavior is ethical because the tool will be used to create a better virus scanner.
B. The behavior is ethical because any experienced programmer could create such a tool.
C. The behavior is not ethical because creating any kind of virus is bad.
D. The behavior is not ethical because such a tool could be leaked on the Internet.

Correct Answer: A
Section:

QUESTION 68

Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

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

Correct Answer: B
Section:

QUESTION 69
Which of the following statements is TRUE for point-to-point microwave transmissions?

A. They are not subject to interception due to encryption.
B. Interception only depends on signal strength.
C. They are too highly multiplexed for meaningful interception.
D. They are subject to interception by an antenna within proximity.

Correct Answer: D
Section:

QUESTION 70
The key benefits of a signed and encrypted e-mail include

A. confidentiality, authentication, and authorization.
B. confidentiality, non-repudiation, and authentication.
C. non-repudiation, authorization, and authentication.
D. non-repudiation, confidentiality, and authorization.

Correct Answer: B
Section:

QUESTION 71
Copyright provides protection for which of the following?

A. Ideas expressed in literary works
B. A particular expression of an idea
C. New and non-obvious inventions
D. Discoveries of natural phenomena

Correct Answer: B
Section:

QUESTION 72
Which of the following is TRUE about Disaster Recovery Plan (DRP) testing?

A. Operational networks are usually shut down during testing.

B. Testing should continue even if components of the test fail.
C. The company is fully prepared for a disaster if all tests pass.
D. Testing should not be done until the entire disaster plan can be tested.

Correct Answer: B
Section:

QUESTION 73
Which of the following is the FIRST step of a penetration test plan?

A. Analyzing a network diagram of the target network
B. Notifying the company's customers
C. Obtaining the approval of the company's management
D. Scheduling the penetration test during a period of least impact

Correct Answer: C
Section:

QUESTION 74
Which of the following actions should be performed when implementing a change to a database schema in a production system?

A. Test in development, determine dates, notify users, and implement in production
B. Apply change to production, run in parallel, finalize change in production, and develop a back-out strategy
C. Perform user acceptance testing in production, have users sign off, and finalize change
D. Change in development, perform user acceptance testing, develop a back-out strategy, and implement change

Correct Answer: D
Section:

QUESTION 75
Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?

A. Data compression
B. Data classification
C. Data warehousing
D. Data validation

Correct Answer: D
Section:

QUESTION 76
The BEST method of demonstrating a company's security level to potential customers is

A. a report from an external auditor.
B. responding to a customer's security questionnaire.
C. a formal report from an internal auditor.
D. a site visit by a customer's security team.

Correct Answer: A
Section:

QUESTION 77
Which of the following does Temporal Key Integrity Protocol (TKIP) support?

A. Multicast and broadcast messages
B. Coordination of IEEE 802.11 protocols
C. Wired Equivalent Privacy (WEP) systems
D. Synchronization of multiple devices

Correct Answer: C
Section:

QUESTION 78
The stringency of an Information Technology (IT) security assessment will be determined by the

A. system's past security record.
B. size of the system's database.
C. sensitivity of the system's datA.
D. age of the system.

Correct Answer: C
Section:

QUESTION 79
What should be the INITIAL response to Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts?

A. Ensure that the Incident Response Plan is available and current.
B. Determine the traffic's initial source and block the appropriate port.
C. Disable or disconnect suspected target and source systems.
D. Verify the threat and determine the scope of the attack.

Correct Answer: D
Section:

QUESTION 80
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

A. monthly.
B. quarterly.
C. annually.
D. bi-annually.

Correct Answer: C
Section:

QUESTION 81
Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?

A. Simple Mail Transfer Protocol (SMTP) blacklist
B. Reverse Domain Name System (DNS) lookup
C. Hashing algorithm
D. Header analysis

Correct Answer: D
Section:

QUESTION 82
During an audit of system management, auditors find that the system administrator has not been trained. What actions need to be taken at once to ensure the integrity of systems?

A. A review of hiring policies and methods of verification of new employees
B. A review of all departmental procedures
C. A review of all training procedures to be undertaken
D. A review of all systems by an experienced administrator

Correct Answer: D
Section:

QUESTION 83
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

A. As part of the SLA renewal process
B. Prior to a planned security audit
C. Immediately after a security breach
D. At regularly scheduled meetings

Correct Answer: D
Section:

QUESTION 84
Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

A. Test before the IT Audit
B. Test when environment changes
C. Test after installation of security patches
D. Test after implementation of system patches

Correct Answer: B
Section:

QUESTION 85
Which of the following MUST be done when promoting a security awareness program to senior management?

A. Show the need for security; identify the message and the audience
B. Ensure that the security presentation is designed to be all-inclusive
C. Notify them that their compliance is mandatory
D. Explain how hackers have enhanced information security

Correct Answer: D
Section:

QUESTION 86
Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

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

Correct Answer: A
Section:

QUESTION 87
A disadvantage of an application filtering firewall is that it can lead to

A. a crash of the network as a result of user activities.
B. performance degradation due to the rules applied.
C. loss of packets on the network due to insufficient bandwidth.
D. Internet Protocol (IP) spoofing by hackers.

Correct Answer: B
Section:

QUESTION 88
What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

A. Evaluating the efficiency of the plan
B. Identifying the benchmark required for restoration
C. Validating the effectiveness of the plan
D. Determining the Recovery Time Objective (RTO)

Correct Answer: C
Section:

QUESTION 89
Following the completion of a network security assessment, which of the following can BEST be demonstrated?

A. The effectiveness of controls can be accurately measured
B. A penetration test of the network will fail
C. The network is compliant to industry standards

D. All unpatched vulnerabilities have been identified

Correct Answer: A
Section:

QUESTION 90
Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

A. reduce the detected object temperature in relation to the background temperature.
B. increase the detected object temperature in relation to the background temperature.
C. automatically compensate for variance in background temperature.
D. detect objects of a specific temperature independent of the background temperature.

Correct Answer: C
Section:

QUESTION 91
The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

A. data integrity.
B. defense in depth.
C. data availability.
D. non-repudiation.

Correct Answer: B
Section:

QUESTION 92
An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems.
Which of the following MUST be verified by the Information Security Department?

A. The service provider's policies are consistent with ISO/IEC27001 and there is evidence that the service provider is following those policies.
B. The service provider will segregate the data within its systems and ensure that each region's policies are met.
C. The service provider will impose controls and protections that meet or exceed the current systems controls and produce audit logs as verification.
D. The service provider's policies can meet the requirements imposed by the new environment even if they differ from the organization's current policies.

Correct Answer: D
Section:

QUESTION 93
Which of the following is an appropriate source for test data?

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

Correct Answer: D
Section:

QUESTION 94
What is the FIRST step in developing a security test and its evaluation?

A. Determine testing methods
B. Develop testing procedures
C. Identify all applicable security requirements
D. Identify people, processes, and products not in compliance

Correct Answer: C
Section:

QUESTION 95
How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?

A. Take another backup of the media in question then delete all irrelevant operating system files.
B. Create a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level.
C. Generate a message digest (MD) or secure hash on the drive image to detect tampering of the media being examined.
D. Discard harmless files for the operating system, and known installed programs.

Correct Answer: B
Section:

QUESTION 96
Which one of the following is a threat related to the use of web-based client side input validation?

A. Users would be able to alter the input after validation has occurred
B. The web server would not be able to validate the input after transmission
C. The client system could receive invalid input from the web server
D. The web server would not be able to receive invalid input from the client

Correct Answer: A
Section:

QUESTION 97
To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

A. Multiple-pass overwriting
B. Degaussing
C. High-level formatting
D. Physical destruction

Correct Answer: C
Section:

QUESTION 98
Multi-threaded applications are more at risk than single-threaded applications to

A. race conditions.
B. virus infection.
C. packet sniffing.
D. database injection.

Correct Answer: A
Section:

QUESTION 99
Which of the following is a potential risk when a program runs in privileged mode?

A. It may serve to create unnecessary code complexity
B. It may not enforce job separation duties
C. It may create unnecessary application hardening
D. It may allow malicious code to be inserted

Correct Answer: D
Section:

QUESTION 100
The goal of software assurance in application development is to

A. enable the development of High Availability (HA) systems.
B. facilitate the creation of Trusted Computing Base (TCB) systems.
C. prevent the creation of vulnerable applications.
D. encourage the development of open source applications.

Correct Answer: C
Section:

QUESTION 101
What is the ultimate objective of information classification?

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

Correct Answer: B
Section:

QUESTION 102
In a financial institution, who has the responsibility for assigning the classification to a piece of information?

A. Chief Financial Officer (CFO)
B. Chief Information Security Officer (CISO)
C. Originator or nominated owner of the information
D. Department head responsible for ensuring the protection of the information

Correct Answer: C
Section:

QUESTION 103
An organization is designing a large enterprise-wide document repository system. They plan to have several different classification level areas with increasing levels of controls. The BEST way to ensure document confidentiality in the repository is to

A. encrypt the contents of the repository and document any exceptions to that requirement.
B. utilize Intrusion Detection System (IDS) set drop connections if too many requests for documents are detected.
C. keep individuals with access to high security areas from saving those documents into lower security areas.
D. require individuals with access to the system to sign Non-Disclosure Agreements (NDA).

Correct Answer: A
Section:

QUESTION 104
What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

A. Signature
B. Inference
C. Induction
D. Heuristic

Correct Answer: D
Section:

QUESTION 105
Contingency plan exercises are intended to do which of the following?

A. Train personnel in roles and responsibilities
B. Validate service level agreements
C. Train maintenance personnel
D. Validate operation metrics

Correct Answer: A
Section:

QUESTION 106
Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

A. Write a Service Level Agreement (SLA) for the two companies.
B. Set up a Virtual Private Network (VPN) between the two companies.

C. Configure a firewall at the perimeter of each of the two companies.
D. Establish a File Transfer Protocol (FTP) connection between the two companies.

Correct Answer: B
Section:

QUESTION 107
Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

A. Interface with the Public Key Infrastructure (PKI)
B. Improve the quality of security software
C. Prevent Denial of Service (DoS) attacks
D. Establish a secure initial state

Correct Answer: D
Section:

QUESTION 108
What a patch management program?

A. Perform automatic deployment of patches.
B. Monitor for vulnerabilities and threats.
C. Prioritize vulnerability remediation.
D. Create a system inventory.

Correct Answer: D
Section:

QUESTION 109
Which of the following is an open standard for exchanging authentication and authorization data between parties?

A. Wired markup language
B. Hypertext Markup Language (HTML)
C. Extensible Markup Language (XML)
D. Security Assertion Markup Language (SAML)

Correct Answer: D
Section:

QUESTION 110
When designing a networked Information System (IS) where there will be several different types of individual access, what is the FIRST step that should be taken to ensure all access control requirements are addressed?

A. Create a user profile.
B. Create a user access matrix.
C. Develop an Access Control List (ACL).
D. Develop a Role Based Access Control (RBAC) list.

Correct Answer: B
Section:

QUESTION 111
Which of the following is the BEST way to verify the integrity of a software patch?

A. Cryptographic checksums
B. Version numbering
C. Automatic updates
D. Vendor assurance

Correct Answer: A
Section:

QUESTION 112
Which of the following is considered best practice for preventing e-mail spoofing?

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

Correct Answer: B
Section:

QUESTION 113
Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

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

Correct Answer: D
Section:

QUESTION 114
What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

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

Correct Answer: A
Section:

QUESTION 115
The Hardware Abstraction Layer (HAL) is implemented in the

A. system software.
B. system hardware.
C. application software.
D. network hardware.

Correct Answer: A
Section:

QUESTION 116
A security professional has just completed their organization's Business Impact Analysis (BIA).
Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

A. Identify and select recovery strategies.
B. Present the findings to management for funding.
C. Select members for the organization's recovery teams.
D. Prepare a plan to test the organization's ability to recover its operations.

Correct Answer: A
Section:

QUESTION 117
A vulnerability test on an Information System (IS) is conducted to

A. exploit security weaknesses in the IS.
B. measure system performance on systems with weak security controls.
C. evaluate the effectiveness of security controls.
D. prepare for Disaster Recovery (DR) planning.

Correct Answer: C
Section:

QUESTION 118
Who must approve modifications to an organization's production infrastructure configuration?

A. Technical management
B. Change control board
C. System operations
D. System users

Correct Answer: B
Section:

QUESTION 119
When implementing controls in a heterogeneous end-point network for an organization, it is critical that

A. hosts are able to establish network communications.
B. users can make modifications to their security software configurations.
C. common software security components be implemented across all hosts.
D. firewalls running on each host are fully customizable by the user.

Correct Answer: C
Section:

QUESTION 120
Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?

A. Immediately document the finding and report to senior management.
B. Use system privileges to alter the permissions to secure the server
C. Continue the testing to its completion and then inform IT management
D. Terminate the penetration test and pass the finding to the server management team

Correct Answer: A
Section:

QUESTION 121
Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

A. Trusted Platform Module (TPM)
B. Preboot eXecution Environment (PXE)
C. Key Distribution Center (KDC)
D. Simple Key-Management for Internet Protocol (SKIP)

Correct Answer: A
Section:

QUESTION 122
The three PRIMARY requirements for a penetration test are

A. A defined goal, limited time period, and approval of management
B. A general objective, unlimited time, and approval of the network administrator
C. An objective statement, disclosed methodology, and fixed cost
D. A stated objective, liability waiver, and disclosed methodology

Correct Answer: A
Section:

QUESTION 123
Which of the following is an attacker MOST likely to target to gain privileged access to a system?

A. Programs that write to system resources
B. Programs that write to user directories

C. Log files containing sensitive information
D. Log files containing system calls

Correct Answer: A
Section:

QUESTION 124
Why is a system's criticality classification important in large organizations?

A. It provides for proper prioritization and scheduling of security and maintenance tasks.
B. It reduces critical system support workload and reduces the time required to apply patches.
C. It allows for clear systems status communications to executive management.
D. It provides for easier determination of ownership, reducing confusion as to the status of the asset.

Correct Answer: A
Section:

QUESTION 125
By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

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

Correct Answer: B
Section:

QUESTION 126
In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?

A. A full-scale simulation of an emergency and the subsequent response functions
B. A specific test by response teams of individual emergency response functions
C. A functional evacuation of personnel
D. An activation of the backup site

Correct Answer: C
Section:

QUESTION 127
Which of the following does the Encapsulating Security Payload (ESP) provide?

A. Authorization and integrity
B. Availability and integrity
C. Integrity and confidentiality
D. Authorization and confidentiality

Correct Answer: C
Section:

QUESTION 128
Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

A. Role Based Access Control (RBAC)
B. Biometric access control
C. Federated Identity Management (IdM)
D. Application hardening

Correct Answer: A
Section:

QUESTION 129
What is an effective practice when returning electronic storage media to third parties for repair?

A. Ensuring the media is not labeled in any way that indicates the organization's name.
B. Disassembling the media and removing parts that may contain sensitive datA.
C. Physically breaking parts of the media that may contain sensitive datA.
D. Establishing a contract with the third party regarding the secure handling of the mediA.

Correct Answer: D
Section:

QUESTION 130
A Business Continuity Plan (BCP) is based on

A. the policy and procedures manual.
B. an existing BCP from a similar organization.
C. a review of the business processes and procedures.
D. a standard checklist of required items and objectives.

Correct Answer: D
Section:

QUESTION 131
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

A. Temporal Key Integrity Protocol (TKIP)
B. Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK)
C. Wi-Fi Protected Access 2 (WPA2) Enterprise
D. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

Correct Answer: C
Section:

QUESTION 132
A thorough review of an organization's audit logs finds that a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient. What type of attack has MOST likely occurred?

A. Spoofing
B. Eavesdropping
C. Man-in-the-middle
D. Denial of service

Correct Answer: C
Section:

QUESTION 133
Which of the following is the MOST effective attack against cryptographic hardware modules?

A. Plaintext
B. Brute force
C. Power analysis
D. Man-in-the-middle (MITM)

Correct Answer: C
Section:

QUESTION 134
Which of the following is the MOST difficult to enforce when using cloud computing?

A. Data access
B. Data backup
C. Data recovery
D. Data disposal

Correct Answer: D
Section:

QUESTION 135
Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?

A. Testing with a Botnet
B. Testing with an EICAR file
C. Executing a binary shellcode
D. Run multiple antivirus programs

Correct Answer: B
Section:

QUESTION 136
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

A. Use a thumb drive to transfer information from a foreign computer.
B. Do not take unnecessary information, including sensitive information.
C. Connect the laptop only to well-known networks like the hotel or public Internet cafes.
D. Request international points of contact help scan the laptop on arrival to ensure it is protected.

Correct Answer: B
Section:

QUESTION 137
Which of the following assures that rules are followed in an identity management architecture?

A. Policy database
B. Digital signature
C. Policy decision point
D. Policy enforcement point

Correct Answer: D
Section:

QUESTION 138
Which of the following violates identity and access management best practices?

A. User accounts
B. System accounts
C. Generic accounts
D. Privileged accounts

Correct Answer: C
Section:

QUESTION 139
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

A. Perform a service provider PCI-DSS assessment on a yearly basis.
B. Validate the service provider's PCI-DSS compliance status on a regular basis.
C. Validate that the service providers security policies are in alignment with those of the organization.
D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis.

Correct Answer: B
Section:

QUESTION 140
What is the MAIN feature that onion routing networks offer?

A. Non-repudiation
B. Traceability

C. Anonymity
D. Resilience

Correct Answer: C
Section:

QUESTION 141
Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

A. Secondary use of the data by business users
B. The organization's security policies and standards
C. The business purpose for which the data is to be used
D. The overall protection of corporate resources and data

Correct Answer: B
Section:

QUESTION 142
Which of the following methods provides the MOST protection for user credentials?

A. Forms-based authentication
B. Digest authentication
C. Basic authentication
D. Self-registration

Correct Answer: B
Section:

QUESTION 143
Which of the following MOST influences the design of the organization's electronic monitoring policies?

A. Workplace privacy laws
B. Level of organizational trust
C. Results of background checks
D. Business ethical considerations

Correct Answer: A
Section:

QUESTION 144
Without proper signal protection, embedded systems may be prone to which type of attack?

A. Brute force
B. Tampering
C. Information disclosure
D. Denial of Service (DoS)

Correct Answer: C
Section:

QUESTION 145
Which of the following is a detective access control mechanism?

A. Log review
B. Least privilege
C. Password complexity
D. Non-disclosure agreement

Correct Answer: A
Section:

QUESTION 146
Which of the following BEST describes Recovery Time Objective (RTO)?

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

Correct Answer: C
Section:

QUESTION 147
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. Availability
B. Confidentiality
C. Integrity
D. Ownership

Correct Answer: A
Section:

QUESTION 148
An online retail company has formulated a record retention schedule for customer transactions.
Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

A. Pending legal hold
B. Long term data mining needs
C. Customer makes request to retain
D. Useful for future business initiatives

Correct Answer: A

Section:

QUESTION 149

Which of the following is the MAIN goal of a data retention policy?

A. Ensure that data is destroyed properly.

B. Ensure that data recovery can be done on the datA.

C. Ensure the integrity and availability of data for a predetermined amount of time.

D. Ensure the integrity and confidentiality of data for a predetermined amount of time.

Correct Answer: C

Section:

QUESTION 150

Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?

A. Resource Servers are required to use passwords to authenticate end users.

B. Revocation of access of some users of the third party instead of all the users from the third party.

C. Compromise of the third party means compromise of all the users in the service.

D. Guest users need to authenticate with the third party identity provider.

Correct Answer: A

Section:

QUESTION 151

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

A. Legal

B. Logical

C. Physical

D. Procedural

Correct Answer: C

Section:

QUESTION 152

Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

A. Masquerading, salami, malware, polymorphism

B. Brute force, dictionary, phishing, keylogger

C. Zeus, netbus, rabbit, turtle

D. Token, biometrics, IDS, DLP

Correct Answer: B

Section:

QUESTION 153

Which of the following is an example of two-factor authentication?

A. Retina scan and a palm print
B. Fingerprint and a smart card
C. Magnetic stripe card and an ID badge
D. Password and Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)

Correct Answer: B
Section:

QUESTION 154
Which item below is a federated identity standard?

A. 802.11i
B. Kerberos
C. Lightweight Directory Access Protocol (LDAP)
D. Security Assertion Markup Language (SAML)

Correct Answer: D
Section:

QUESTION 155
What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?

A. Some users are not provisioned into the service.
B. SAML tokens are provided by the on-premise identity provider.
C. Single users cannot be revoked from the service.
D. SAML tokens contain user information.

Correct Answer: A
Section:

QUESTION 156
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive email, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following could have MOST likely prevented the Peer-to-Peer (P2P) program from being installed on the computer?

A. Removing employee's full access to the computer
B. Supervising their child's use of the computer
C. Limiting computer's access to only the employee
D. Ensuring employee understands their business conduct guidelines

Correct Answer: A
Section:

QUESTION 157

Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive email, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?

A. Anti-virus software
B. Intrusion Prevention System (IPS)
C. Anti-spyware software
D. Integrity checking software

Correct Answer: B
Section:

QUESTION 158
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive email, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?

A. Run software uninstall
B. Re-image the computer
C. Find and remove all installation files
D. Delete all cookies stored in the web browser cache

Correct Answer: B
Section:

QUESTION 159
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive email, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following documents explains the proper use of the organization's assets?

A. Human resources policy
B. Acceptable use policy
C. Code of ethics
D. Access control policy

Correct Answer: B
Section:

QUESTION 160
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In the plan, what is the BEST approach to mitigate future internal client-based attacks?

A. Block all client side web exploits at the perimeter.

B. Remove all non-essential client-side web services from the network.
C. Screen for harmful exploits of client-side services before implementation.
D. Harden the client image before deployment.

Correct Answer: D
Section:

QUESTION 161
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?

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

Correct Answer: D
Section:

QUESTION 162
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
What MUST the plan include in order to reduce client-side exploitation?

A. Approved web browsers
B. Network firewall procedures
C. Proxy configuration
D. Employee education

Correct Answer: D
Section:

QUESTION 163
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
What is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?

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

Correct Answer: C
Section:

QUESTION 164

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

A. Least privilege
B. Lattice Based Access Control (LBAC)
C. Role Based Access Control (RBAC)
D. Lightweight Directory Access Control (LDAP)

Correct Answer: C
Section:

QUESTION 165
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session.
Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
In addition to authentication at the start of the user session, best practice would require reauthentication

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

Correct Answer: D
Section:

QUESTION 166
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session.
Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Following best practice, where should the permitted access for each department and job classification combination be specified?

A. Security procedures
B. Security standards
C. Human resource policy
D. Human resource standards

Correct Answer: B
Section:

QUESTION 167
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session.
Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The

organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
What MUST the access control logs contain in addition to the identifier?

A. Time of the access
B. Security classification
C. Denied access attempts
D. Associated clearance

Correct Answer: A
Section:

QUESTION 168
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Which of the following is considered the MOST important priority for the information security officer?

A. Formal acceptance of the security strategy
B. Disciplinary actions taken against unethical behavior
C. Development of an awareness program for new employees
D. Audit of all organization system configurations for faults

Correct Answer: A
Section:

QUESTION 169
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The effectiveness of the security program can PRIMARILY be measured through

A. audit findings.
B. risk elimination.
C. audit requirements.
D. customer satisfaction.

Correct Answer: A
Section:

QUESTION 170
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

A. Severity of risk
B. Complexity of strategy

C. Frequency of incidents

D. Ongoing awareness

Correct Answer: A
Section:

QUESTION 171
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program.
There are numerous initiatives requiring security involvement.
The security program can be considered effective when

A. vulnerabilities are proactively identified.

B. audits are regularly performed and reviewed.

C. backups are regularly performed and validated.

D. risk is lowered to an acceptable level.

Correct Answer: D
Section:

QUESTION 172
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?

A. Unauthorized database changes

B. Integrity of security logs

C. Availability of the database

D. Confidentiality of the incident

Correct Answer: A
Section:

QUESTION 173
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

A. Availability

B. Integrity

C. Accountability

D. Confidentiality

Correct Answer: D
Section:

QUESTION 174
Refer to the information below to answer the question.

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If the intrusion causes the system processes to hang, which of the following has been affected?

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

Correct Answer: B
Section:

QUESTION 175
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will be the PRIMARY security concern as staff is released from the organization?

A. Inadequate IT support
B. Loss of data and separation of duties
C. Undocumented security controls
D. Additional responsibilities for remaining staff

Correct Answer: B
Section:

QUESTION 176
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will MOST likely allow the organization to keep risk at an acceptable level?

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

Correct Answer: C
Section:

QUESTION 177
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will indicate where the IT budget is BEST allocated during this time?

A. Policies
B. Frameworks

C. Metrics
D. Guidelines

Correct Answer: C
Section:

QUESTION 178
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
When determining appropriate resource allocation, which of the following is MOST important to monitor?

A. Number of system compromises
B. Number of audit findings
C. Number of staff reductions
D. Number of additional assets

Correct Answer: B
Section:

QUESTION 179
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

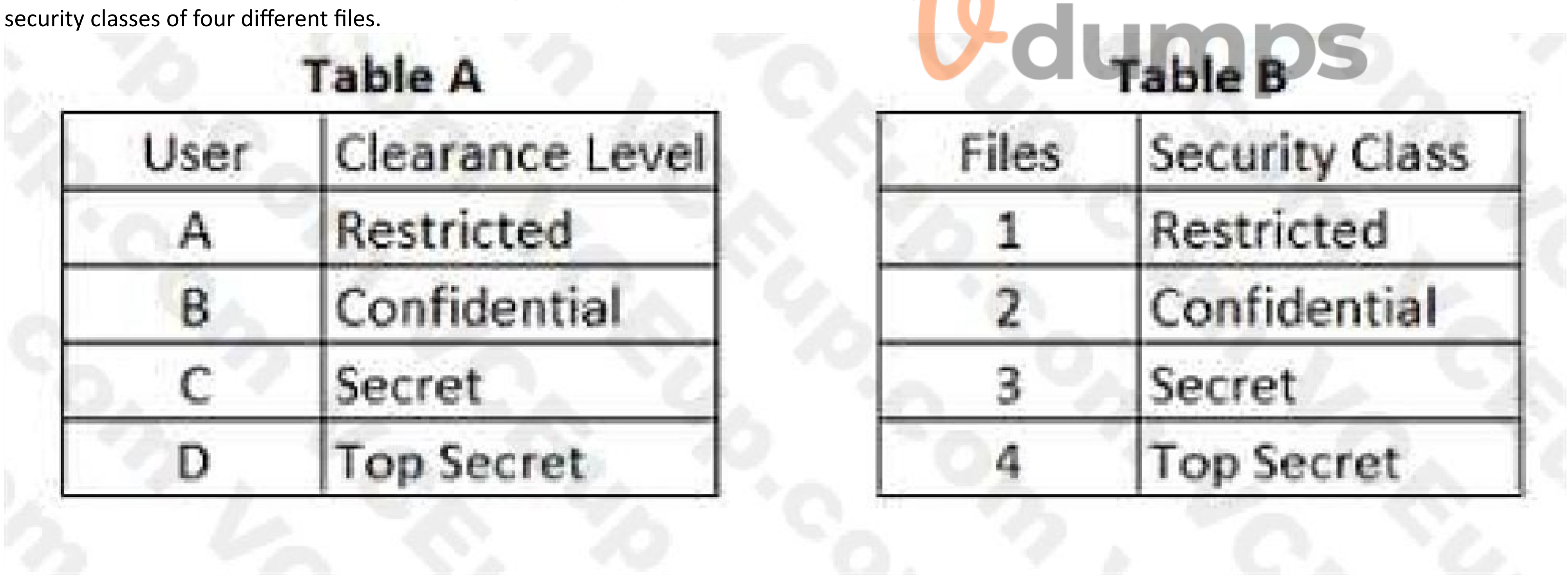


Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

Which of the following is true according to the star property (*property)?

A. User D can write to File 1
B. User B can write to File 1
C. User A can write to File 1
D. User C can write to File 1

Correct Answer: C
Section:

QUESTION 180

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

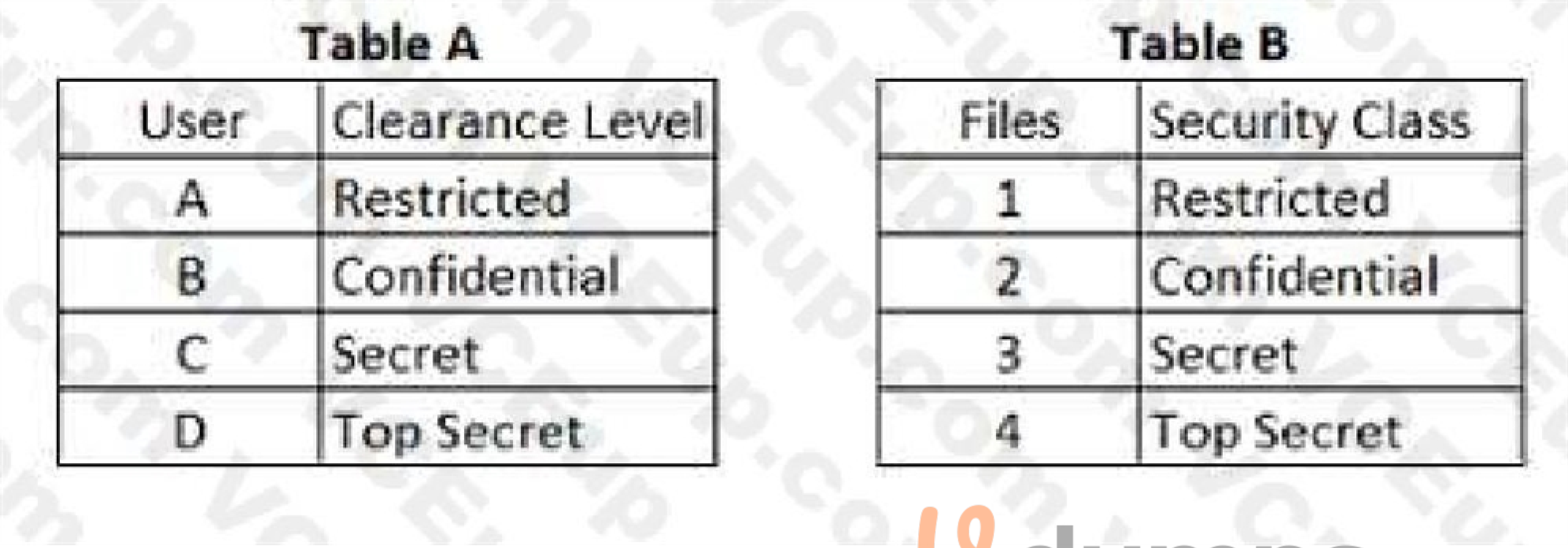


Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

In a Bell-LaPadula system, which user cannot write to File 3?

A. User A
B. User B
C. User C
D. User D

Correct Answer: D
Section:

QUESTION 181

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

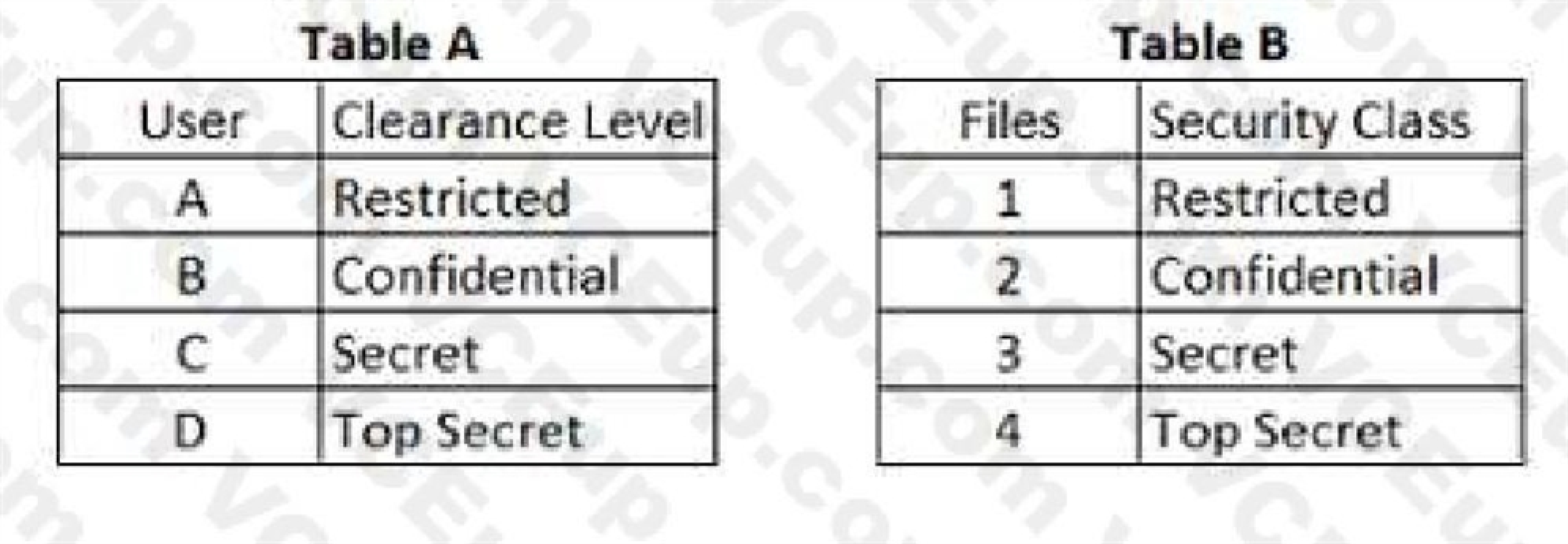


Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

In a Bell-LaPadula system, which user has the MOST restrictions when writing data to any of the four files?

A. User A
B. User B
C. User C
D. User D

Correct Answer: D
Section:

QUESTION 182
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

A. Commercial products often have serious weaknesses of the magnetic force available in the degausser product.
B. Degausser products may not be properly maintained and operated.
C. The inability to turn the drive around in the chamber for the second pass due to human error.
D. Inadequate record keeping when sanitizing mediA.

Correct Answer: B
Section:

QUESTION 183
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?

A. Knurling
B. Grinding
C. Shredding
D. Degaussing

Correct Answer: C
Section:

QUESTION 184
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The third party needs to have

A. processes that are identical to that of the organization doing the outsourcing.
B. access to the original personnel that were on staff at the organization.
C. the ability to maintain all of the applications in languages they are familiar with.
D. access to the skill sets consistent with the programming languages used by the organization.

Correct Answer: D
Section:

QUESTION 185
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The organization should ensure that the third party's physical security controls are in place so that they

A. are more rigorous than the original controls.
B. are able to limit access to sensitive information.
C. allow access by the organization staff at any time.
D. cannot be accessed by subcontractors of the third party.

Correct Answer: B
Section:

QUESTION 186
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
What additional considerations are there if the third party is located in a different country?

A. The organizational structure of the third party and how it may impact timelines within the organization
B. The ability of the third party to respond to the organization in a timely manner and with accurate information
C. The effects of transborder data flows and customer expectations regarding the storage or processing of their data
D. The quantity of data that must be provided to the third party and how it is to be used

Correct Answer: C
Section:

QUESTION 187
What is the MOST critical factor to achieve the goals of a security program?

A. Capabilities of security resources
B. Executive management support
C. Effectiveness of security management
D. Budget approved for security resources

Correct Answer: B
Section:

QUESTION 188
A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

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

Correct Answer: C
Section:

QUESTION 189
During an audit, the auditor finds evidence of potentially illegal activity. Which of the following is the MOST appropriate action to take?

A. Immediately call the police
B. Work with the client to resolve the issue internally
C. Advise the person performing the illegal activity to cease and desist
D. Work with the client to report the activity to the appropriate authority

Correct Answer: D
Section:

QUESTION 190
Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

A. Timing
B. Cold boot
C. Side channel
D. Acoustic cryptanalysis

Correct Answer: B
Section:

QUESTION 191
What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

A. Identify regulatory requirements
B. Conduct a risk assessment
C. Determine business drivers
D. Review the security baseline configuration

Correct Answer: B
Section:

QUESTION 192
Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

A. Set up a BIOS and operating system password
B. Encrypt the virtual drive where confidential files can be stored
C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
D. Encrypt the entire disk and delete contents after a set number of failed access attempts

Correct Answer: D
Section:

QUESTION 193
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

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

Correct Answer: A
Section:

QUESTION 194
What component of a web application that stores the session state in a cookie can be bypassed by an attacker?

A. An initialization check
B. An identification check
C. An authentication check
D. An authorization check

Correct Answer: C
Section:

QUESTION 195
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

A. Use of a unified messaging.
B. Use of separation for the voice network.
C. Use of Network Access Control (NAC) on switches.
D. Use of Request for Comments (RFC) 1918 addressing.

Correct Answer: A
Section:

QUESTION 196
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

A. Automatically create exceptions for specific actions or files
B. Determine which files are unsafe to access and blacklist them
C. Automatically whitelist actions or files known to the system
D. Build a baseline of normal or safe system events for review

Correct Answer: D
Section:

QUESTION 197
Which of the following describes the concept of a Single Sign -On (SSO) system?

A. Users are authenticated to one system at a time.
B. Users are identified to multiple systems with several credentials.
C. Users are authenticated to multiple systems with one login.
D. Only one user is using the system at a time.

Correct Answer: C
Section:

QUESTION 198
What physical characteristic does a retinal scan biometric device measure?

A. The amount of light reflected by the retina
B. The size, curvature, and shape of the retina
C. The pattern of blood vessels at the back of the eye
D. The pattern of light receptors at the back of the eye

Correct Answer: C
Section:

QUESTION 199
What does secure authentication with logging provide?

A. Data integrity
B. Access accountability
C. Encryption logging format

D. Segregation of duties

Correct Answer: B
Section:

QUESTION 200
Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

A. Access based on rules
B. Access based on user's role
C. Access determined by the system
D. Access based on data sensitivity

Correct Answer: B
Section:

QUESTION 201
Discretionary Access Control (DAC) restricts access according to

A. data classification labeling.
B. page views within an application.
C. authorizations granted to the user.
D. management accreditation.

Correct Answer: C
Section:

QUESTION 202
Retaining system logs for six months or longer can be valuable for what activities?

A. Disaster recovery and business continuity
B. Forensics and incident response
C. Identity and authorization management
D. Physical and logical access control

Correct Answer: B
Section:

QUESTION 203
Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?

A. It is useful for testing communications protocols and graphical user interfaces.
B. It is characterized by the stateless behavior of a process implemented in a function.
C. Test inputs are obtained from the derived threshold of the given functional specifications.
D. An entire partition can be covered by considering only one representative value from that partition.

Correct Answer: C

Section:

QUESTION 204
Data leakage of sensitive information is MOST often concealed by which of the following?

A. Secure Sockets Layer (SSL)
B. Secure Hash Algorithm (SHA)
C. Wired Equivalent Privacy (WEP)
D. Secure Post Office Protocol (POP)

Correct Answer: A
Section:

QUESTION 205
Which of the following is a reason to use manual patch installation 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 likelihood of system or application incompatibilities will be decreased.
D. The ability to cover large geographic areas is increased.

Correct Answer: C
Section:

QUESTION 206
Which of the following is the MOST important element of change management documentation?

A. List of components involved
B. Number of changes being made
C. Business case justification
D. A stakeholder communication

Correct Answer: C
Section:

QUESTION 207
The PRIMARY outcome of a certification process is that it provides documented

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

Correct Answer: D
Section:

QUESTION 208

Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. International Organization for Standardization (ISO) 27000 family
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standard (PCIDSS)
D. ISO/IEC 20000

Correct Answer: A
Section:

QUESTION 209
Which of the following PRIMARILY contributes to security incidents in web-based applications?

A. Systems administration and operating systems
B. System incompatibility and patch management
C. Third-party applications and change controls
D. Improper stress testing and application interfaces

Correct Answer: C
Section:

QUESTION 210
What is the process called when impact values are assigned to the security objectives for information types?

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

Correct Answer: D
Section:

QUESTION 211
Data remanence refers to which of the following?

A. The remaining photons left in a fiber optic cable after a secure transmission.
B. The retention period required by law or regulation.
C. The magnetic flux created when removing the network connection from a server or personal computer.
D. The residual information left on magnetic storage media after a deletion or erasure.

Correct Answer: D
Section:

QUESTION 212
Which of the following describes the BEST configuration management practice?

A. After installing a new system, the configuration files are copied to a separate back-up system and hashed to detect tampering.

B. After installing a new system, the configuration files are copied to an air-gapped system and hashed to detect tampering.
C. The firewall rules are backed up to an air-gapped system.
D. A baseline configuration is created and maintained for all relevant systems.

Correct Answer: D
Section:

QUESTION 213
How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?

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

Correct Answer: B
Section:

QUESTION 214
Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

A. Ineffective data classification
B. Lack of data access controls
C. Ineffective identity management controls
D. Lack of Data Loss Prevention (DLP) tools

Correct Answer: A
Section:

QUESTION 215
A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.
Which of the following is the BEST location?

A. On the top floor
B. In the basement
C. In the core of the building
D. In an exterior room with windows

Correct Answer: C
Section:

QUESTION 216
Which of the following is the PRIMARY concern when using an Internet browser to access a cloudbased service?

A. Insecure implementation of Application Programming Interfaces (API)
B. Improper use and storage of management keys
C. Misconfiguration of infrastructure allowing for unauthorized access

D. Vulnerabilities within protocols that can expose confidential data

Correct Answer: D
Section:

QUESTION 217
After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

A. Implement strong passwords authentication for VPN
B. Integrate the VPN with centralized credential stores
C. Implement an Internet Protocol Security (IPSec) client
D. Use two-factor authentication mechanisms

Correct Answer: D
Section:

QUESTION 218
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

A. Challenge response and private key
B. Digital certificates and Single Sign-On (SSO)
C. Tokens and passphrase
D. Smart card and biometrics

Correct Answer: D
Section:

QUESTION 219
If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this result?

A. User error
B. Suspected tampering
C. Accurate identification
D. Unsuccessful identification

Correct Answer: B
Section:

QUESTION 220
Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

A. Security control baselines, access controls, employee awareness and training
B. Human resources, asset management, production management
C. Supply chain lead time, inventory control, encryption
D. Polygraphs, crime statistics, forensics

Correct Answer: A
Section:

QUESTION 221
Discretionary Access Control (DAC) is based on which of the following?

A. Information source and destination
B. Identification of subjects and objects
C. Security labels and privileges
D. Standards and guidelines

Correct Answer: B
Section:

QUESTION 222
By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

A. Lock pinging
B. Lock picking
C. Lock bumping
D. Lock bricking

Correct Answer: B
Section:

QUESTION 223
An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.
As part of the authentication process, which of the following must the end user provide?

A. An access token
B. A username and password
C. A username
D. A password

Correct Answer: A
Section:

QUESTION 224
How does an organization verify that an information system's current hardware and software match the standard system configuration?

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

Correct Answer: C

Section:

QUESTION 225

The goal of a Business Continuity Plan (BCP) training and awareness program is to

A. enhance the skills required to create, maintain, and execute the plan.
B. provide for a high level of recovery in case of disaster.
C. describe the recovery organization to new employees.
D. provide each recovery team with checklists and procedures.

Correct Answer: A
Section:

QUESTION 226

Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

A. Read-through
B. Parallel
C. Full interruption
D. Simulation

Correct Answer: D
Section:

QUESTION 227

An organization has developed a major application that has undergone accreditation testing. After receiving the results of the evaluation, what is the final step before the application can be accredited?

A. Acceptance of risk by the authorizing official
B. Remediation of vulnerabilities
C. Adoption of standardized policies and procedures
D. Approval of the System Security Plan (SSP)

Correct Answer: A
Section:

QUESTION 228

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

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

Correct Answer: B
Section:

QUESTION 229

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

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

Correct Answer: A
Section:

QUESTION 230
What does an organization FIRST review to assure compliance with privacy requirements?

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

Correct Answer: C
Section:

QUESTION 231
Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?

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

Correct Answer: B
Section:

QUESTION 232
An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?

A. Application Manager
B. Database Administrator
C. Privacy Officer
D. Finance Manager

Correct Answer: C
Section:

QUESTION 233
Which of the following analyses is performed to protect information assets?

A. Business impact analysis

B. Feasibility analysis
C. Cost benefit analysis
D. Data analysis

Correct Answer: A
Section:

QUESTION 234
Which of the following methods can be used to achieve confidentiality and integrity for data in transit?

A. Multiprotocol Label Switching (MPLS)
B. Internet Protocol Security (IPSec)
C. Federated identity management
D. Multi-factor authentication

Correct Answer: B
Section:

QUESTION 235
Secure Sockets Layer (SSL) encryption protects

A. data at rest.
B. the source IP address.
C. data transmitted.
D. data availability.

Correct Answer: C
Section:

QUESTION 236
Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

A. Concept, Development, Production, Utilization, Support, Retirement
B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
C. Acquisition, Measurement, Configuration Management, Production, Operation, Support
D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Correct Answer: B
Section:

QUESTION 237
Which of the following BEST describes a Protection Profile (PP)?

A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
B. A document that is used to develop an IT security product from its security requirements definition.
C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

Correct Answer: A
Section:

QUESTION 238
Which of the following BEST describes a rogue Access Point (AP)?

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

Correct Answer: C
Section:

QUESTION 239
The 802.1x standard provides a framework for what?

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

Correct Answer: B
Section:

QUESTION 240
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

A. Confidentiality and Integrity
B. Availability and Accountability
C. Integrity and Availability
D. Accountability and Assurance

Correct Answer: D
Section:

QUESTION 241
Which of the following is the PRIMARY security concern associated with the implementation of smart cards?

A. The cards have limited memory
B. Vendor application compatibility
C. The cards can be misplaced
D. Mobile code can be embedded in the card

Correct Answer: C
Section:

QUESTION 242
Which of the following is a function of Security Assertion Markup Language (SAML)?

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

Correct Answer: D
Section:

QUESTION 243
What is an important characteristic of Role Based Access Control (RBAC)?

A. Supports Mandatory Access Control (MAC)
B. Simplifies the management of access rights
C. Relies on rotation of duties
D. Requires two factor authentication

Correct Answer: B
Section:

QUESTION 244
A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

A. Static discharge
B. Consumption
C. Generation
D. Magnetism

Correct Answer: B
Section:

QUESTION 245
Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

A. Verify countermeasures have been deactivated.
B. Ensure firewall logging has been activated.
C. Validate target systems have been backed up.
D. Confirm warm site is ready to accept connections.

Correct Answer: C
Section:

QUESTION 246
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

A. Policy documentation review
B. Authentication validation
C. Periodic log reviews
D. Interface testing

Correct Answer: C
Section:

QUESTION 247
What is the GREATEST challenge of an agent-based patch management solution?

A. Time to gather vulnerability information about the computers in the program
B. Requires that software be installed, running, and managed on all participating computers
C. The significant amount of network bandwidth while scanning computers
D. The consistency of distributing patches to each participating computer

Correct Answer: B
Section:

QUESTION 248
Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

A. security impact analysis.
B. structured code review.
C. routine self assessment.
D. cost benefit analysis.

Correct Answer: A
Section:

QUESTION 249
Disaster Recovery Plan (DRP) training material should be

A. consistent so that all audiences receive the same training.
B. stored in a fire proof safe to ensure availability when needed.
C. only delivered in paper format.
D. presented in a professional looking manner.

Correct Answer: A
Section:

QUESTION 250
The MAIN reason an organization conducts a security authorization process is to

A. force the organization to make conscious risk decisions.
B. assure the effectiveness of security controls.
C. assure the correct security organization exists.

D. force the organization to enlist management support.

Correct Answer: A
Section:

QUESTION 251
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?

A. Document the system as high risk
B. Perform a vulnerability assessment
C. Perform a quantitative threat assessment
D. Notate the information and move on

Correct Answer: B
Section:

QUESTION 252
The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the

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

Correct Answer: A
Section:

QUESTION 253
What is the GREATEST challenge to identifying data leaks?

A. Available technical tools that enable user activity monitoring.
B. Documented asset classification policy and clear labeling of assets.
C. Senior management cooperation in investigating suspicious behavior.
D. Law enforcement participation to apprehend and interrogate suspects.

Correct Answer: B
Section:

QUESTION 254
While investigating a malicious event, only six days of audit logs from the last month were available.
What policy should be updated to address this problem?

A. Retention

B. Reporting
C. Recovery
D. Remediation

Correct Answer: A
Section:

QUESTION 255
Who is ultimately responsible to ensure that information assets are categorized and adequate measures are taken to protect them?

A. Data Custodian
B. Executive Management
C. Chief Information Security Officer
D. Data/Information/Business Owners

Correct Answer: B
Section:

QUESTION 256
A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

A. Onward transfer
B. Collection Limitation
C. Collector Accountability
D. Individual Participation

Correct Answer: B
Section:

QUESTION 257
Which of the following is the PRIMARY benefit of implementing data-in-use controls?

A. If the data is lost, it must be decrypted to be opened.
B. If the data is lost, it will not be accessible to unauthorized users.
C. When the data is being viewed, it can only be printed by authorized users.
D. When the data is being viewed, it must be accessed using secure protocols.

Correct Answer: C
Section:

QUESTION 258
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

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

Correct Answer: A
Section:

QUESTION 259
Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?

A. Level of assurance of the Target of Evaluation (TOE) in intended operational environment
B. Selection to meet the security objectives stated in test documents
C. Security behavior expected of a TOE
D. Definition of the roles and responsibilities

Correct Answer: C
Section:

QUESTION 260
Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?

A. IEEE 802.1F
B. IEEE 802.1H
C. IEEE 802.1Q
D. IEEE 802.1X

Correct Answer: D
Section:

QUESTION 261
The PRIMARY security concern for handheld devices is the

A. strength of the encryption algorithm.
B. spread of malware during synchronization.
C. ability to bypass the authentication mechanism.
D. strength of the Personal Identification Number (PIN).

Correct Answer: C
Section:

QUESTION 262
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Authorizations are not included in the server response
B. Unsalted hashes are passed over the network
C. The authentication session can be replayed
D. Passwords are passed in cleartext

Correct Answer: D
Section:

QUESTION 263
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:

QUESTION 264
Which of the following would BEST describe the role directly responsible for data within an organization?

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

Correct Answer: A
Section:

QUESTION 265
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:

QUESTION 266
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:

QUESTION 267
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: C
Section:

QUESTION 268
During which of the following processes is least privilege implemented for a user account?

A. Provision
B. Approve
C. Request
D. Review

Correct Answer: A
Section:

QUESTION 269
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:

QUESTION 270
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
Section:

QUESTION 271
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:

QUESTION 272
In which identity management process is the subject's identity established?

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

Correct Answer: D
Section:

QUESTION 273
In order to assure authenticity, which of the following are required?

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

Correct Answer: D
Section:

QUESTION 274
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:

QUESTION 275
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: B
Section:

QUESTION 276
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:

QUESTION 277
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 organizational policy.

Correct Answer: D
Section:

QUESTION 278
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:

QUESTION 279
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:

QUESTION 280
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:

QUESTION 281
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:

QUESTION 282
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:

QUESTION 283
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:

QUESTION 284
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:

QUESTION 285
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:

QUESTION 286
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:

QUESTION 287
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:

QUESTION 288
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:

QUESTION 289
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:

QUESTION 290
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:

QUESTION 291
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:

QUESTION 292
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:

QUESTION 293

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: B
Section:

QUESTION 294

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:

QUESTION 295

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:

QUESTION 296

When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

A. Countermeasure effectiveness
B. Type of potential loss
C. Incident likelihood
D. Information ownership

Correct Answer: C
Section:

QUESTION 297

A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements. Which of the following BEST minimizes the risk of this happening again?

A. Define additional security controls directly after the merger

B. Include a procurement officer in the merger team

C. Verify all contracts before a merger occurs

D. Assign a compliancy officer to review the merger conditions

Correct Answer: D
Section:

QUESTION 298
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:

QUESTION 299
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:

QUESTION 300
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:

QUESTION 301
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: B
Section:

QUESTION 302
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

A. Log all activities associated with sensitive systems
B. Provide links to security policies
C. Confirm that confidentially agreements are signed
D. Employ strong access controls

Correct Answer: D
Section:

QUESTION 303
Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

A. Erase
B. Sanitize
C. Encrypt
D. Degauss

Correct Answer: B
Section:

QUESTION 304
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: D
Section:

QUESTION 305
Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

A. Inert gas fire suppression system
B. Halon gas fire suppression system

C. Dry-pipe sprinklers
D. Wet-pipe sprinklers

Correct Answer: A
Section:

QUESTION 306
Unused space in a disk cluster is important in media analysis because it may contain which of the following?

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

Correct Answer: A
Section:

QUESTION 307
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:

QUESTION 308
Which of the following is MOST appropriate for protecting confidentially of data stored on a hard drive?

A. Triple Data Encryption Standard (3DES)
B. Advanced Encryption Standard (AES)
C. Message Digest 5 (MD5)
D. Secure Hash Algorithm 2(SHA-2)

Correct Answer: B
Section:

QUESTION 309
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:

QUESTION 310
What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

A. Non-repudiation
B. Efficiency
C. Confidentially
D. Privacy

Correct Answer: A
Section:

QUESTION 311
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
D. Encrypt removable USB devices containing data at rest

Correct Answer: C
Section:

QUESTION 312
Which of the following MUST be in place to recognize a system attack?

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

Correct Answer: C
Section:

QUESTION 313
Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

A. Integration using Lightweight Directory Access Protocol (LDAP)
B. Form-based user registration process
C. Integration with the organizations Human Resources (HR) system
D. A considerably simpler provisioning process

Correct Answer: D
Section:

QUESTION 314
Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

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

Correct Answer: A
Section:

QUESTION 315
A minimal 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: B
Section:

QUESTION 316
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:

QUESTION 317
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:

QUESTION 318
Why is planning in Disaster Recovery (DR) an interactive process?

A. It details off-site storage plans
B. It identifies omissions in the plan
C. It defines the objectives of the plan
D. It forms part of the awareness process

Correct Answer: C
Section:

QUESTION 319
Mandatory Access Controls (MAC) are based on:

A. security classification and security clearance
B. data segmentation and data classification
C. data labels and user access permissions
D. user roles and data encryption

Correct Answer: A
Section:

QUESTION 320
What is the foundation of cryptographic functions?

A. Encryption
B. Cipher
C. Hash
D. Entropy

Correct Answer: D
Section:

QUESTION 321
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?

A. 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:

QUESTION 322
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:

QUESTION 323
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
Section:

QUESTION 324
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: C
Section:

QUESTION 325
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:

QUESTION 326
Which of the following is part of a Trusted Platform Module (TPM)?

A. A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion
B. A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for "measuring" the state of a computing platform
C. A secure processor targeted at managing digital keys and accelerating digital signing
D. A platform-independent software interface for accessing computer functions

Correct Answer: A
Section:

QUESTION 327
In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

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

Correct Answer: A
Section:

QUESTION 328
Which of the following combinations would MOST negatively affect availability?

A. Denial of Service (DoS) attacks and outdated hardware
B. Unauthorized transactions and outdated hardware
C. Fire and accidental changes to data
D. Unauthorized transactions and denial of service attacks

Correct Answer: A
Section:

QUESTION 329
Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

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

Correct Answer: B
Section:

QUESTION 330
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: A
Section:

QUESTION 331
Which of the following is a characteristic of an internal audit?

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

Correct Answer: D
Section:

QUESTION 332
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.
D. Ensure that data decisions and impacts are communicated to the organization.

Correct Answer: A
Section:

QUESTION 333
What is the MAIN goal of information security awareness and training?

A. To inform users of the latest malware threats
B. To inform users of information assurance responsibilities
C. To comply with the organization information security policy
D. To prepare students for certification

Correct Answer: B
Section:

QUESTION 334
Proven application security principles include which of the following?

A. Minimizing attack surface area
B. Hardening the network perimeter
C. Accepting infrastructure security controls
D. Developing independent modules

Correct Answer: A
Section:

QUESTION 335
When developing a business case for updating a security program, the security program owner MUST do which of the following?

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

Correct Answer: A
Section:

QUESTION 336
From a security perspective, which of the following assumptions MUST be made about input to an application?

A. It is tested
B. It is logged
C. It is verified
D. It is untrusted

Correct Answer: D
Section:

QUESTION 337
Which of the following is the BEST reason for writing an information security policy?

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

Correct Answer: A
Section:

QUESTION 338
What is the PRIMARY goal of fault tolerance?

A. Elimination of single point of failure
B. Isolation using a sandbox
C. Single point of repair
D. Containment to prevent propagation

Correct Answer: A
Section:

QUESTION 339
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:

QUESTION 340
Which one of the following data integrity models assumes a lattice of integrity levels?

A. Take-Grant
B. Biba
C. Harrison-Ruzzo
D. Bell-LaPadula

Correct Answer: B
Section:

QUESTION 341
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

Correct Answer: A
Section:

QUESTION 342
Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

A. Minimize malicious attacks from third parties
B. Manage resource privileges
C. Share digital identities in hybrid cloud
D. Defined a standard protocol

Correct Answer: B
Section:

QUESTION 343
An organization has discovered that users are visiting unauthorized websites using anonymous proxies.
Which of the following is the BEST way to prevent future occurrences?

A. Remove the anonymity from the proxy
B. Analyze Internet Protocol (IP) traffic for proxy requests
C. Disable the proxy server on the firewall
D. Block the Internet Protocol (IP) address of known anonymous proxies

Correct Answer: D
Section:

QUESTION 344
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: C
Section:

QUESTION 345
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: D
Section:

QUESTION 346
Due to system constraints, a group of system administrators must share a high-level access set of credentials.
Which of the following would be MOST appropriate to implement?

A. Increased console lockout times for failed logon attempts
B. Reduce the group in size
C. A credential check-out process for a per-use basis
D. Full logging on affected systems

Correct Answer: C
Section:

QUESTION 347
Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency 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 exitdoor
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:

QUESTION 348

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:

QUESTION 349

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

A. Chief Information Officer (CIO)

B. Chief Information Security Officer (CISO)

C. Chief internal auditor

D. Chief Executive Officer (CEO)

Correct Answer: B

Section:

QUESTION 350

A security analyst for a large financial institution is reviewing network traffic related to an incident.

The analyst determines the traffic is irrelevant to the investigation but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user's desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst's next step?

A. Send the log file co-workers for peer review

B. Include the full network traffic logs in the incident report

C. Follow organizational processes to alert the proper teams to address the issue.

D. Ignore data as it is outside the scope of the investigation and the analyst's role.

Correct Answer: C

Section:

QUESTION 351

An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies.

What code of ethics canon is being observed?

A. Provide diligent and competent service to principals

B. Protect society, the commonwealth, and the infrastructure

C. Advance and protect the profession

D. Act honorable, honesty, justly, responsibly, and legally

Correct Answer: A

Section:

QUESTION 352
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: A
Section:

QUESTION 353
What is the MAIN purpose of a change management policy?

A. To assure management that changes to the Information Technology (IT) infrastructure are necessary
B. To identify the changes that may be made to the Information Technology (IT) infrastructure
C. To verify that changes to the Information Technology (IT) infrastructure are approved
D. To determine the necessary for implementing modifications to the Information Technology (IT) infrastructure

Correct Answer: C
Section:

QUESTION 354
Who is responsible for the protection of information when it is shared with or provided to other organizations?

A. Systems owner
B. Authorizing Official (AO)
C. Information owner
D. Security officer

Correct Answer: C
Section:

QUESTION 355
Which of the following is the MOST challenging issue in apprehending cyber criminals?

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

Correct Answer: C
Section:

QUESTION 356

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:

QUESTION 357
Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

A. undergo a security assessment as part of authorization process
B. establish a risk management strategy
C. harden the hosting server, and perform hosting and application vulnerability scans
D. establish policies and procedures on system and services acquisition

Correct Answer: D
Section:

QUESTION 358
An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

A. The Data Protection Authority (DPA)
B. The Cloud Service Provider (CSP)
C. The application developers
D. The data owner

Correct Answer: B
Section:

QUESTION 359
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:

QUESTION 360
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:

QUESTION 361
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:

QUESTION 362
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:

QUESTION 363
Which of the following is the MOST important security goal when performing application interface testing?

A. Confirm that all platforms are supported and function properly

B. Evaluate whether systems or components pass data and control correctly to one another

C. Verify compatibility of software, hardware, and network connections

D. Examine error conditions related to external interfaces to prevent application details leakage

Correct Answer: B
Section:

QUESTION 364
Which of the following is the MOST common method of memory protection?

A. Compartmentalization

B. Segmentation

C. Error correction

D. Virtual Local Area Network (VLAN) tagging

Correct Answer: B
Section:

QUESTION 365
Attack trees are MOST useful for which of the following?

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

Correct Answer: C
Section:

QUESTION 366
Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

A. Automated dynamic analysis
B. Automated static analysis
C. Manual code review
D. Fuzzing

Correct Answer: A
Section:

QUESTION 367
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: A
Section:

QUESTION 368
The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

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

Correct Answer: B

Section:

QUESTION 369
What is the BEST location in a network to place Virtual Private Network (VPN) devices when an internal review reveals network design flaws in remote access?

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

Correct Answer: B
Section:

QUESTION 370
Which of the following access management procedures would minimize the possibility of an organization's employees retaining access to secure werk areas after they change roles?

A. User access modification
B. user access recertification
C. User access termination
D. User access provisioning

Correct Answer: B
Section:

QUESTION 371
What Is the FIRST step in establishing an information security program?

A. Establish an information security policy.
B. Identify factors affecting information security.
C. Establish baseline security controls.
D. Identify critical security infrastructure.

Correct Answer: A
Section:

QUESTION 372
Which of the following is MOST effective in detecting information hiding in Transmission Control Protocol/internet Protocol (TCP/IP) traffic?

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

Correct Answer: A
Section:

QUESTION 373

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

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

Correct Answer: C
Section:

QUESTION 374
Which of the following is the BEST Identity-as-a-Service (IDaaS) solution for validating users?

A. Single Sign-On (SSO)
B. Security Assertion Markup Language (SAML)
C. Lightweight Directory Access Protocol (LDAP)
D. Open Authentication (OAuth)

Correct Answer: B
Section:

QUESTION 375
When conducting a security assessment of access controls, which activity is part of the data analysis phase?

A. Present solutions to address audit exceptions.
B. Conduct statistical sampling of data transactions.
C. Categorize and identify evidence gathered during the audit.
D. Collect logs and reports.

Correct Answer: C
Section:

QUESTION 376
Which of the following is used to support the of defense in depth during development phase of a software product?

A. Security auditing
B. Polyinstantiation
C. Maintenance
D. Known vulnerability list

Correct Answer: B
Section:

QUESTION 377
When a system changes significantly, who is PRIMARILY responsible for assessing the security impact?

A. Chief Information Security Officer (CISO)

B. Information System Owner
C. Information System Security Officer (ISSO)
D. Authorizing Official

Correct Answer: B
Section:

QUESTION 378
When selecting a disk encryption technology, which of the following MUST also be assured to be encrypted?

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

Correct Answer: A
Section:

QUESTION 379
Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

A. Watering hole
B. Brute force
C. Spear phishing
D. Address Resolution Protocol (ARP) poisoning

Correct Answer: D
Section:

QUESTION 380
Additional padding may be added to toe Encapsulating Security Protocol (ESP) b trailer to provide which of the following?

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

Correct Answer: C
Section:

QUESTION 381
Company A is evaluating new software to replace an in-house developed application. During the acquisition process. Company A specified the security retirement, as well as the functional requirements. Company B responded to the acquisition request with their flagship product that runs on an Operating System (OS) that Company A has never used nor evaluated. The flagship product meets all security -and functional requirements as defined by Company A.
Based upon Company B's response, what step should Company A take?

A. Move ahead with the acpjisition process, and purchase the flagship software

B. Conduct a security review of the OS
C. Perform functionality testing
D. Enter into contract negotiations ensuring Service Level Agreements (SLA) are established to include security patching

Correct Answer: B
Section:

QUESTION 382
What is maintained by using write blocking devices whan forensic evidence is examined?

A. Inventory
B. lntegrity
C. Confidentiality
D. Availability

Correct Answer: B
Section:

QUESTION 383
Which of the following is a characteristic of a challenge/response authentication process?

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

Correct Answer: C
Section:

QUESTION 384
Which of the following is the PRIMARY risk associated with Extensible Markup Language (XML) applications?

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

Correct Answer: A
Section:

QUESTION 385
Activity to baseline, tailor, and scope security controls tikes place dring which National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) step?

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

Correct Answer: D
Section:

QUESTION 386
A large corporation is locking for a solution to automate access based on where on request is coming from, who the user is, what device they are connecting with, and what time of day they are attempting this access. What type of solution would suit their needs?

A. Discretionary Access Control (DAC)
B. Role Based Access Control (RBAC)
C. Mandater Access Control (MAC)
D. Network Access Control (NAC)

Correct Answer: D
Section:

QUESTION 387
Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

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

Correct Answer: C
Section:

QUESTION 388
When adopting software as a service (Saas), which security responsibility will remain with remain with the adopting organization?

A. Physical security
B. Data classification
C. Network control
D. Application layer control

Correct Answer: B
Section:

QUESTION 389
Secure real-time transport protocol (SRTP) provides security for which of the following?

A. time sensitive e-communication
B. Voice communication
C. Satellite communication
D. Network Communication for real-time operating systems

Correct Answer: B
Section:

QUESTION 390
Which of the following authorization standards is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM)?

A. Security Assertion Markup Language (SAML)
B. Open Authentication (OAUTH)
C. Remote Authentication Dial-in User service (RADIUS)
D. Terminal Access Control Access Control System Plus (TACACS+)

Correct Answer: B
Section:

QUESTION 391
Which programming methodology allows a programmer to use pre-determined blocks of code end consequently reducing development time and programming costs?

A. Application security
B. Object oriented
C. Blocked algorithm
D. Assembly language

Correct Answer: B
Section:

QUESTION 392
Why do certificate Authorities (CA) add value to the security of electronic commerce transactions?

A. They maintain the certificate revocation list.
B. They maintain the private keys of transition parties.
C. They verify the transaction parties' private keys.
D. They provide a secure communication enamel to the transaction parties.

Correct Answer: D
Section:

QUESTION 393
If a content management system (CSM) is implemented, which one of the following would occur?

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

Correct Answer: A
Section:

QUESTION 394
During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should en assessor do?

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

Correct Answer: A
Section:

QUESTION 395
Which of the following is an accurate statement when an assessment results in the discovery of vulnerabilities in a critical network component?

A. The fact that every other host is sufficiently hardened does not change the fact frat the network is placed at risk of attack.
B. There is little likelihood that the entire network is being placed at a significant risk of attack.
C. A second assessment should immediately be performed after all vulnerabilities are corrected.
D. There is a low possibility that any adjacently connected components have been compromised by an attacker

Correct Answer: C
Section:

QUESTION 396
What technique used for spoofing the origin of an email can successfully conceal the sender s Internet Protocol (IP) address?

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

Correct Answer: C
Section:

QUESTION 397
What is a warn site when conducting Business continuity planning (BCP)

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

Correct Answer: B
Section:

QUESTION 398
Which of the following four iterative steps are conducted on third-party vendors in an on-going basis?

A. Investigate, Evaluate, Respond, Monitor
B. Frame, Assess, Respond, Monitor
C. Frame, Assess, Remediate, Monitor

D. Investigate, Assess, Remediate, Monitor

Correct Answer: C
Section:

QUESTION 399
Which of the following media is least problematic with data remanence?

A. Magnetic disk
B. Electrically Erasable Programming read-only Memory (EEPROM)
C. Dynamic Random Access Memory (DRAM)
D. Flash memory

Correct Answer: C
Section:

QUESTION 400
During a recent assessment an organization has discovered that the wireless signal can be detected outside the campus are a. What logical control should be implemented in order to BFST protect One confidentiality of information traveling
One wireless transmission media?

A. Configure a firewall to logically separate the data at the boundary.
B. Configure the Access Points (AP) to use Wi-Fi Protected Access 2 (WPA2) encryption.
C. Disable the Service Set Identifier (SSID) broadcast on the Access Points (AP).
D. Perform regular technical assessments on the Wireless Local Area Network (WLAN).

Correct Answer: B
Section:

QUESTION 401
Who is essential for developing effective test scenarios for disaster recovery (DR) test plans?

A. Business line management and IT staff members
B. Chief Information Officer (CIO) and DR manager
C. DR manager end IT staff members
D. IT staff members and project managers

Correct Answer: B
Section:

QUESTION 402
Which is the second phase of public key Infrastructure (pk1) key/certificate life-cycle management?

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

Correct Answer: C
Section:

QUESTION 403
Which of the following is MOST important when determining appropriate countermeasures for an identified risk?

A. Interaction with existing controls
B. Cost
C. Organizational risk tolerance
D. Patch availability

Correct Answer: C
Section:

QUESTION 404
When a flaw in Industrial control (ICS) software is discovered, what is the GREATEST impediment to deploying a patch?

A. Many IG systems have software that is no longer being maintained by the venders.
B. Compensating controls may impact IG performance.
C. Testing a patch in an IG may require more resources than the organization can commit.
D. vendors are required to validate the operability patches.

Correct Answer: D
Section:

QUESTION 405
Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information form malicious software?

A. Analyze the behavior of the program.
B. Examine the file properties and permissions.
C. Review the code to identify its origin.
D. Analyze the logs generated by the software.

Correct Answer: A
Section:

QUESTION 406
In fault-tolerant systems, what do rollback capabilities permit?

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

Correct Answer: A
Section:

QUESTION 407
How does identity as a service (IDaaS) provide an easy mechanism for integrating identity service into individual applications with minimal development effort?

A. By allowing the identification logic and storage of an identity's attributes to be maintained externally
B. By integrating internal provisioning procedures with external authentication processes
C. By allowing for internal provisioning of user accounts
D. By keeping all user information in easily accessible cloud repositories

Correct Answer: D
Section:

QUESTION 408
A security practitioner has been tasked with establishing organizational asset handling procedures.
What should be considered that would have the GRFATEST impact to the development of these procedures?

A. Media handling procedures
B. User roles and responsibilities
C. Acceptable Use Policy (ALP)
D. Information classification scheme

Correct Answer: D
Section:

QUESTION 409
From an asset security perspective, what is the BEST countermeasure to prevent data theft due to data remanence when a sensitive data storage media is no longer needed?

A. Return the media to the system owner.
B. Delete the sensitive data from the media.
C. Physically destroy the retired media.
D. Encrypt data before it Is stored on the media.

Correct Answer: C
Section:

QUESTION 410
A project requires the use of en authentication mechanism where playback must be protected and plaintext secret must be used. Which of the following should be used?

A. Password Authentication Protocol (PAP)
B. Extensible Authentication Protocol (EAP)
C. Secure Hash Algorithm (SHA)
D. Challenge Handshake Authentication Protocol (CHAP)

Correct Answer: A
Section:

QUESTION 411
Which of the following threats exists with an implementation of digital signatures?

A. Spoofing
B. Substitution
C. Content tampering
D. Eavesdropping

Correct Answer: A
Section:

QUESTION 412
What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

A. Resumption procedures describing the actions to be taken to return to normal business operations
B. Emergency procedures describing the necessary actions to be taken following an incident jeopardizes business operations
C. Fallback procedures describing what action are to be taken to more essential business activities to alternative temporary locations
D. Maintain schedule how and the plan will be tested and the process for maintaining the plan

Correct Answer: B
Section:

QUESTION 413
When deploying en Intrusion Detection System (IDS) on a high-volume network, the need to distribute the load across multiple sensors would create which technical problem?

A. Session continuity
B. Proxy authentication failure
C. Sensor overload
D. Synchronized sensor updates

Correct Answer: A
Section:

QUESTION 414
How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

A. Use a Virtual Local Area Network (VLAN) to segment the network
B. Implement a bastion host
C. Install anti-virus on all enceinte
D. Enforce port security on access switches

Correct Answer: A
Section:

QUESTION 415
Which of the following is the MOST important consideration that must be taken into account when deploying an enterprise patching solution that includes mobile devices?

A. Service provider(s) utilized by the organization
B. Whether it will impact personal use

C. Number of mobile users in the organization
D. Feasibility of downloads due to available bandwidth

Correct Answer: C
Section:

QUESTION 416
Which of the following is the weakest form of protection for an application that handles Personally Identifiable Information (PII)?

A. Transport Layer Security (TLS)
B. Ron Rivest Cipher 4 (RC4) encryption
C. Security Assertion Markup Language (SAML)
D. Multifactor authentication

Correct Answer: B
Section:

QUESTION 417
Which is the MOST effective countermeasure to prevent electromagnetic emanations on unshielded data cable?

A. Move cable are away from exterior facing windows
B. Encase exposed cable runs in metal conduit
C. Enable Power over Ethernet (PoE) to increase voltage
D. Bundle exposed cables together to disguise their signals

Correct Answer: B
Section:

QUESTION 418
Which of the following is the MOST significant benefit to implementing a third-party federated identity architecture?

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

Correct Answer: C
Section:

QUESTION 419
A criminal organization is planning an attack on a government network. Which of the following is the MOST severe attack to the network availability?

A. Network management communications is disrupted by attacker
B. Operator loses control of network devices to attacker
C. Sensitive information is gathered on the network topology by attacker
D. Network is flooded with communication traffic by attacker

Correct Answer: B
Section:

QUESTION 420
Limiting the processor, memory, and Input/output (I/O) capabilities of mobile code is known as

A. code restriction.
B. on-demand compile.
C. sandboxing.
D. compartmentalization.

Correct Answer: C
Section:

QUESTION 421
Which of the following security testing strategies is BEST suited for companies with low to moderate security maturity?

A. Load Testing
B. White-box testing
C. Black -box testing
D. Performance testing

Correct Answer: B
Section:

QUESTION 422
Which of the following are core categories of malicious attack against Internet of Things (IOT) devices?

A. Packet capture and false data injection
B. Packet capture and brute force attack
C. Node capture 3nd Structured Query Langue (SQL) injection
D. Node capture and false data injection

Correct Answer: D
Section:

QUESTION 423
Which of the following entails identification of data end links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

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

Correct Answer: A
Section:

QUESTION 424
Which of the following is critical if an employee is dismissed due to violation of an organization's Acceptable Use Policy (ALP)?

A. Privilege suspension
B. Internet access logs
C. Proxy records
D. Appropriate documentation

Correct Answer: B
Section:

QUESTION 425
Which of the following is the PRIMARY security consideration for how an organization should handle Information Technology (IT) assets?

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

Correct Answer: D
Section:

QUESTION 426
In a dispersed network that lacks central control, which of the following is die PRIMARY course of action to mitigate exposure?

A. Implement management policies, audit control, and data backups
B. Implement security policies and standards, access controls, and access limitations
C. Implement security policies and standards, data backups, and audit controls
D. Implement remote access policies, shared workstations, and log management

Correct Answer: C
Section:

QUESTION 427
What are the roles within a scrum methodology?

A. Scrum master, retirements manager, and development team
B. System owner, scrum master, and development team
C. Scrum master, quality assurance team, and scrum team
D. Product owner, scrum master, and scrum team

Correct Answer: D
Section:

QUESTION 428
When conducting a forensic criminal investigation on a computer had drive, what should be dene PRIOR to analysis?

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

Correct Answer: C
Section:

QUESTION 429
Which of the following initiates the systems recovery phase of a disaster recovery plan?

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

Correct Answer: A
Section:

QUESTION 430
Which type of fire alarm system sensor is intended to detect fire at its earliest stage?

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

Correct Answer: A
Section:

QUESTION 431
An organization implements a Remote Access Server (RAS). Once users correct to the server, digital certificates are used to authenticate their identity. What type of Extensible Authentication Protocol (EAP) would the organization use dring this authentication?

A. Transport layer security (TLS)
B. Message Digest 5 (MD5)
C. Lightweight Extensible Authentication Protocol (EAP)
D. Subscriber Identity Module (SIM)

Correct Answer: A
Section:

QUESTION 432
Which of the following MUST a security professional do in order to quantify the value of a security program to organization management?

A. Report using metrics.
B. Rank priorities as high, medium, or low.

C. Communicate compliance obstacles.

D. Report en employee activities

Correct Answer: A
Section:

QUESTION 433
A client has reviewed a vulnerability assessment report and has stated it is Inaccurate. The client states that the vulnerabilities listed are not valid because the host's Operating System (OS) was not properly detected. Where in the vulnerability assessment process did the erra MOST likely occur?

A. Detection

B. Enumeration

C. Reporting

D. Discovery

Correct Answer: A
Section:

QUESTION 434
Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

A. Security credentials

B. Known vulnerabilities

C. Inefficient algorithms

D. Coding mistakes

Correct Answer: A
Section:

QUESTION 435
Which of the following is a common measure within a Local Area Network (LAN) to provide en additional level of security through segmentation?

A. Building Virtual Local Area Networks (VLAN)

B. Building Demilitarized Zones (DMZ)

C. Implementing a virus scanner

D. Implementing an Intrusion Detection System (IDS)

Correct Answer: A
Section:

QUESTION 436
What Is the FIRST step for a digital investigator to perform when using best practices to collect digital evidence from a potential crime scene?

A. Consult the lead investigate to team the details of the case and required evidence.

B. Assure that grounding procedures have been followed to reduce the loss of digital data due to static electricity discharge.

C. Update the Basic Input Output System (BIOS) and Operating System (OS) of any tools used to assure evidence admissibility.

D. Confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims.

Correct Answer: D
Section:

QUESTION 437
How can an attacker exploit overflow to execute arbitrary code?

A. Modify a function's return address.
B. Alter the address of the stack.
C. Substitute elements in the stack.
D. Move the stack pointer.

Correct Answer: A
Section:

QUESTION 438
Which of the following is TRUE regarding equivalence class testing?

A. It is characterized by the stateless behavior of a process implemented In a function.
B. An entire partition can be covered by considering only one representative value from that partition.
C. Test inputs are obtained from the derived boundaries of the given functional specifications.
D. It is useful for testing communications protocols and graphical user interfaces.

Correct Answer: C
Section:

QUESTION 439
Which of the following is the BEST way to protect against structured Query language (SQL) injection?

A. Enforce boundary checking.
B. Restrict use of SELECT command.
C. Restrict Hyper Text Markup Language (HTNL) source code access.
D. Use stored procedures.

Correct Answer: D
Section:

QUESTION 440
Which of the following BEST describes the responsibilities of data owner?

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

Correct Answer: B
Section:

QUESTION 441
Which area of embedded devices are most commonly attacked?

A. Application
B. Firmware
C. Protocol
D. Physical Interface

Correct Answer: A
Section:

QUESTION 442
If virus infection is suspected, which of the following is the FIRST step for the user to take?

A. Unplug the computer from the network.
B. Save the opened files and shutdown the computer.
C. Report the incident to service desk.
D. Update the antivirus to the latest version.

Correct Answer: C
Section:

QUESTION 443
Which of the following MOST applies to session initiation protocal (SIP) security?

A. It leverages Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS).
B. It requires a Public Key Infrastructure (PKI).
C. It reuses security mechanisms derived from existing protocols.
D. It supports end-to-end security natively.

Correct Answer: C
Section:

QUESTION 444
Which layer of the Open systems Interconnection (OSI) model is being targeted in the event of a Synchronization (SYN) flood attack?

A. Session
B. Transport
C. Network
D. Presentation

Correct Answer: B
Section:

QUESTION 445
What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

A. Business Impact Analysis (BIA)
B. Security Assessment Report (SAR)
C. Plan of Action and Milestones {POA&M)
D. Security Assessment Plan (SAP)

Correct Answer: C
Section:

QUESTION 446
When dealing with shared, privilaged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

A. Regularity change the passwords,
B. implement a password vaulting solution.
C. Lock passwords in tamperproof envelopes in a safe.
D. Implement a strict access control policy.

Correct Answer: B
Section:

QUESTION 447
Which of the following actions MUST be performed when using secure multipurpose internet mail Extension (S/MIME) before sending an encrypted message to a recipient?

A. Digitally sign foe message.
B. Obtain the recipients private key.
C. Obtain the recipient's digital certificate.
D. Encrypt attachments.

Correct Answer: A
Section:

QUESTION 448
Which type of test suite should be run for fast feedback during application develoment?

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

Correct Answer: C
Section:

QUESTION 449
What are the roles within a scrum methodoligy?

A. System owner, scrum master, and development team
B. prduct owner, scrum master, and scrum team
C. Scrum master, requirements manager, and development team

D. Scrum master, quality assurance team, and scrum team

Correct Answer: B
Section:

QUESTION 450
What is the FIRST step required in establishing a records retention program?

A. Identify and inventory all records.
B. Identify and inventory all records storage locations
C. Classify records based on sensitivity.
D. Draft a records retention policy.

Correct Answer: D
Section:

QUESTION 451
Which of the following was developed to support multiple protocols as well as provide as well as provide login, password, and error correction capabilities?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Point-to-Point Protocol (PPP)
C. Password Authentication Protocol (PAP)
D. Post Office Protocol (POP)

Correct Answer: A
Section:

QUESTION 452
An organization discovers that its secure file transfer protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization's general information technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.
Which of the following is the MOST probable attack vector used in the security breach?

A. Buffer overflow
B. Weak password able to lack of complexity rules
C. Distributed Denial of Service (DDoS)
D. Cross-Site Scripting (XSS)

Correct Answer: A
Section:

QUESTION 453
If a content management system (CMC) is implemented, which one of the following would occur?

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

Correct Answer: D
Section:

QUESTION 454
Which of the following is the BEST identity-as-a-service (IDaaS) solution for validating users?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAM.)
C. Single Sign-on (SSO)
D. Open Authentication (OAuth)

Correct Answer: A
Section:

QUESTION 455
Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?

A. Session
B. Transport
C. Data Link
D. Network

Correct Answer: B
Section:

QUESTION 456
What is the most effective form of media sanitization to ensure residual data cannot be retrieved?

A. Clearing
B. Destroying
C. Purging
D. Disposal

Correct Answer: B
Section:

QUESTION 457
Why is lexical obfuscation in software development discouraged by many organizations?

A. Problems writing test cases
B. Problems recovering systems after disaster
C. Problems compiling the code
D. Problems maintaining data connections

Correct Answer: C
Section:

QUESTION 458
What steps can be taken to prepare personally identifiable information (PII) for processing by a third party?

A. It is not necessary to protect PII as long as it is in the hands of the provider.
B. A security agreement with a Cloud Service Provider (CSP) was required so there is no concern.
C. The personal information should be maintained separately connected with a one-way reference.
D. The personal information can be hashed and then the data can be sent to an outside processor.

Correct Answer: C
Section:

QUESTION 459
Why are mobile devices something difficult to investigate in a forensic examination?

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

Correct Answer: B
Section:

QUESTION 460
Which of the following is a characteristic of a challenge/response authentication process?

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

Correct Answer: A
Section:

QUESTION 461
Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device Which has stolen?

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

Correct Answer: B
Section:

QUESTION 462
Which of the following will help identify the source internet protocol (IP) address of malware being exected on a computer?

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

Correct Answer: A
Section:

QUESTION 463
Which of the following is critical if an empolyee is dismissed due to violation of an organization's acceptable use policy (Aup) ?

A. Appropriate documentation
B. privilege suspension
C. proxy records
D. Internet access logs

Correct Answer: A
Section:

QUESTION 464
Which of the following findings would MOST likely indicate a high risk in a vulnerability assessment report?

A. Transmission control protocol (TCP) port 443 open
B. Non-standard system naming convention used
C. Unlicensed software installed
D. End of life system detected

Correct Answer: A
Section:

QUESTION 465
Digital certificates used transport Layer security (TLS) support which of the following?

A. Server identify and data confidentially
B. Information input validation
C. Multi-Factor Authentication (MFA)
D. Non-reputation controls and data encryption

Correct Answer: A
Section:

QUESTION 466
Which would result in the GREATEST import following a breach to a cloud environment?

A. The hypervisor host Is poorly seared
B. The same Logical Unit Number (LLN) is used for ail VMs
C. Insufficient network segregation

D. Insufficient hardening of Virtual Machines (VM)

Correct Answer: C
Section:

QUESTION 467
Which of the following in the BEST way to reduce the impact of an externally sourced flood attack?

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

Correct Answer: A
Section:

QUESTION 468
Which of the following methods MOST efficiently manages user accounts when using a third-party cloud-based application and directory solution?

A. Cloud directory
B. Directory synchronization
C. Assurance framework
D. Lightweight Directory Access Protocol (LDAP)

Correct Answer: B
Section:

QUESTION 469
Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

A. Data access control policies
B. Threat modeling
C. Common Criteria (CC)
D. Business Impact Analysis (BIA)

Correct Answer: A
Section:

QUESTION 470
A corporate security policy specifies that all devices on the network must have updated operating system patches and anti-malware software. Which technology should be used to enforce this policy?

A. Network Address Translation (NAT)
B. Stateful Inspection
C. Packet filtering
D. Network Access Control (NAC)

Correct Answer: D

Section:

QUESTION 471
When designing on Occupent Emergency plan (OEP) for United states (US) Federal government facilities, what factor must be considered?

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

Correct Answer: A
Section:

QUESTION 472
Why should Open Web Application Security Project (OWASP) Application Security Verification standards (ASVS) Level 1 be considered a MINIMUM level of protection for any web application?

A. ASVS Level 1 ensures that applications are invulnerable to OWASP top 10 threats.
B. Opportunistic attackers will look for any easily exploitable vulnerable applications.
C. Most regulatory bodies consider ASVS Level 1 as a baseline set of controls for applications.
D. Securing applications at ASVS Level 1 provides adequate protection for sensitive data.

Correct Answer: B
Section:

QUESTION 473
Which of the following controls is the most for a system identified as critical in terms of data and function to the organization?

A. Preventive controls
B. Monitoring control
C. Cost controls
D. Compensating controls

Correct Answer: B
Section:

QUESTION 474
An organization operates a legacy Industrial Control System (ICS) to support its core business service, which carrot be replaced. Its management MUST be performed remotely through an administrative console software, which in tum depends on an old version of the Java Runtime Environment (JPE) known to be vulnerable to a number of attacks, How is this risk BEST managed?

A. Isolate the full ICS by moving It onto its own network segment
B. Air-gap and harden the host used for management purposes
C. Convince the management to decommission the ICS and mitigate to a modem technology
D. Deploy a restrictive proxy between all clients and the vulnerable management station

Correct Answer: B
Section:

QUESTION 475
Which of the following steps is performed during the forensic data analysis phase?

A. Collect known system files
B. search for relevant strings.
C. Create file lists
D. Recover deleted data.

Correct Answer: B
Section:

QUESTION 476
Which of the following practices provides the development of security and identification of threats in designing software?

A. Stakeholder review
B. Requirements review
C. Penetration testing
D. Threat modeling

Correct Answer: D
Section:

QUESTION 477
Which of the following presents the PRIMARY concern to an organization when setting up a federated single sign-on (SSO) solution with another

A. Sending assertions to an identity provider
B. Requesting Identity assertions from the partners domain
C. defining the identity mapping scheme
D. Having the resource provider query the Identity provider

Correct Answer: C
Section:

QUESTION 478
The adoption of an enterprise-wide business continuity program requires Which of the following?

A. Good communication throughout the organization
B. Formation of Disaster Recovery (DP) project team
C. A completed Business Impact Analysis (BIA)
D. Well-documented information asset classification

Correct Answer: D
Section:

QUESTION 479
Which of the following is the MOST important reason for using a chain of custody from?

A. To document those who were In possession of the evidence at every point In time

B. To collect records of all digital forensic professionals working on a case

C. To document collected digital evidence

D. To ensure that digital evidence is not overlooked during the analysis

Correct Answer: A
Section:

QUESTION 480
When conducting a security assessment of access controls , Which activity is port of the data analysis phase?

A. Collect logs and reports.

B. Present solutions to address audit exceptions.

C. Categorize and Identify evidence gathered during the audit

D. Conduct statiscal sampling of data transactions.

Correct Answer: C
Section:

QUESTION 481
The core component of Role Based Access control (RBAC) must be constructed of defined data elements. Which elements are required?

A. Users, permissions, operators, and protected objects

B. Users, rotes, operations, and protected objects

C. Roles, accounts, permissions, and protected objects

D. Roles, operations, accounts, and protected objects

Correct Answer: B
Section:

QUESTION 482
Which of the following should be included in a hardware retention policy?

Which of the following should be included in a hardware retention policy?

A. The use of encryption technology to encrypt sensitive data prior to retention

B. Retention of data for only one week and outsourcing the retention to a third-party vendor

C. Retention of all sensitive data on media and hardware

D. A plan to retain data required only for business purposes and a retention schedule

Correct Answer: A
Section:

QUESTION 483
Individuals have been identified and determined as having a need-to-know for the information.
Which of the following access control methods MUST include a consistent set of rules for controlling and limiting access?

A. Attribute Based Access Control (ABAC)

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

Correct Answer: D
Section:

QUESTION 484
When can a security program be considered effective?

A. Audits are rec/party performed and reviewed.
B. Vulnerabilities are proactively identified.
C. Risk is lowered to an acceptable level.
D. Badges are regulatory performed and validated

Correct Answer: C
Section:

QUESTION 485
Which of the following is the MOST important activity an organization performs to ensure that securiy is part of the overall organization culture?

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

Correct Answer: C
Section:

QUESTION 486
What is the PRIMARY benefit of analyzing the partition layout of a hard disk volume when performing forensic analysis?

A. Sectors which are not assigned to a perform may contain data that was purposely hidden.
B. Volume address information for he hard disk may have been modified.
C. partition tables which are not completely utilized may contain data that was purposely hidden
D. Physical address information for the hard disk may have been modified.

Correct Answer: A
Section:

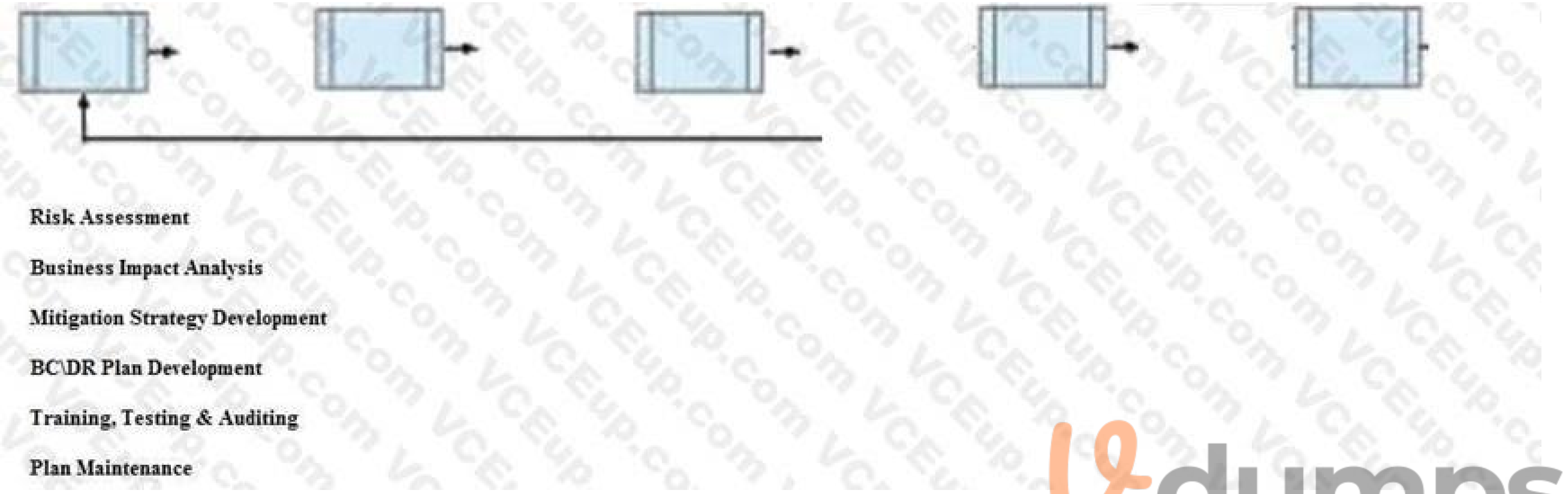
QUESTION 487
Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?

A. SOC 1 Type1
B. SOC 1Type2
C. SOC 2 Type 1
D. SOC 2 Type 2

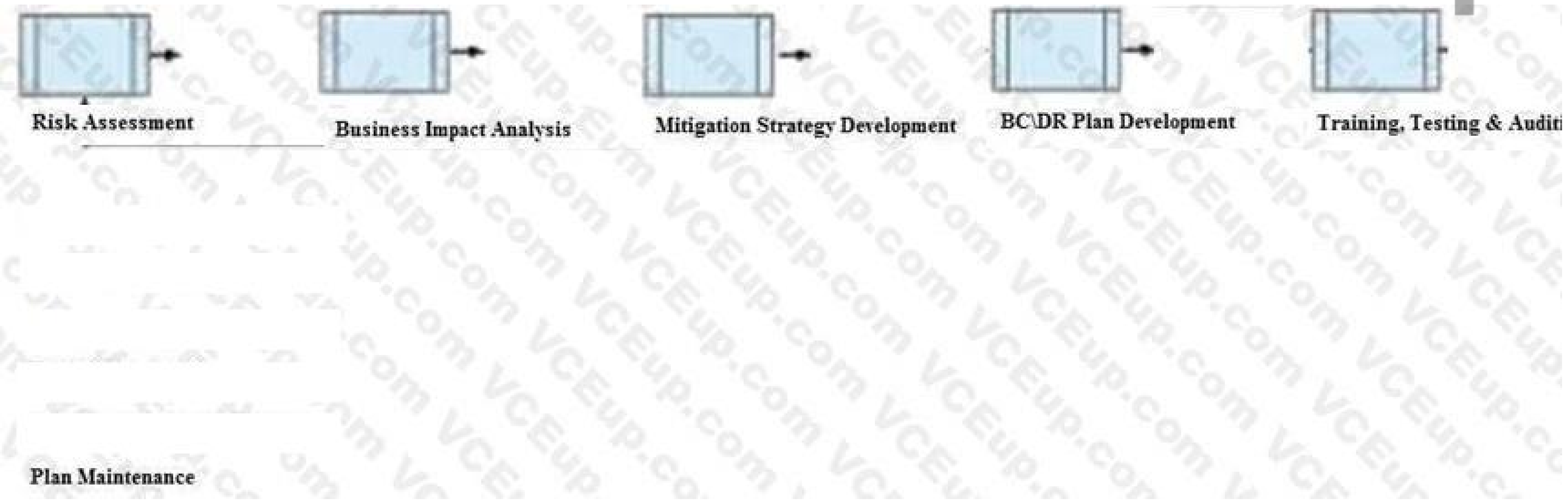
Correct Answer: D
Section:

QUESTION 488
DRAG DROP
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan.
Drag the remaining BC\DR phases to the appropriate corresponding location.

Select and Place:



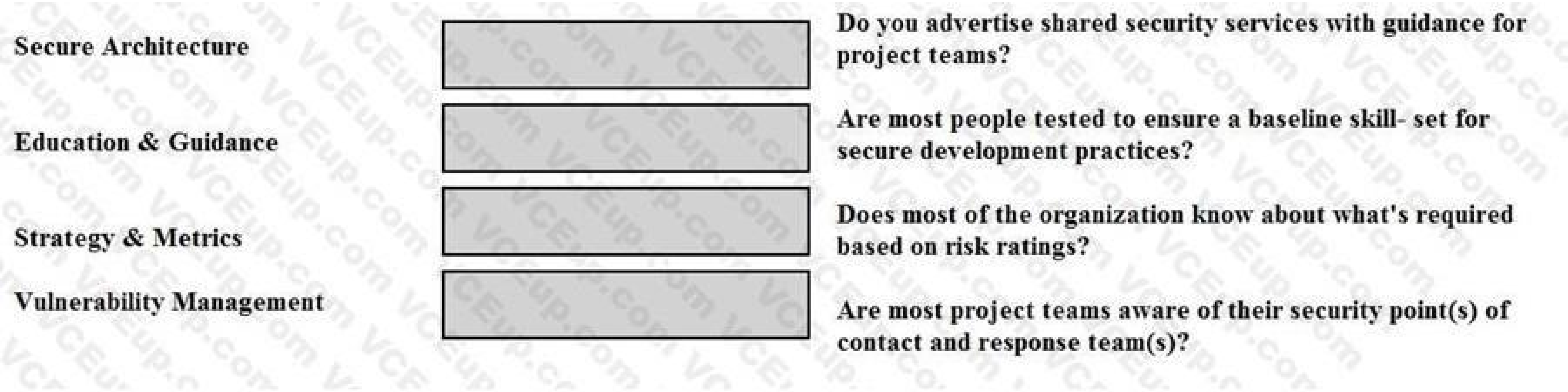
Correct Answer:



Section:
Explanation:

QUESTION 489
DRAG DROP
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

Select and Place:



Secure Architecture

Education & Guidance

Strategy & Metrics

Vulnerability Management

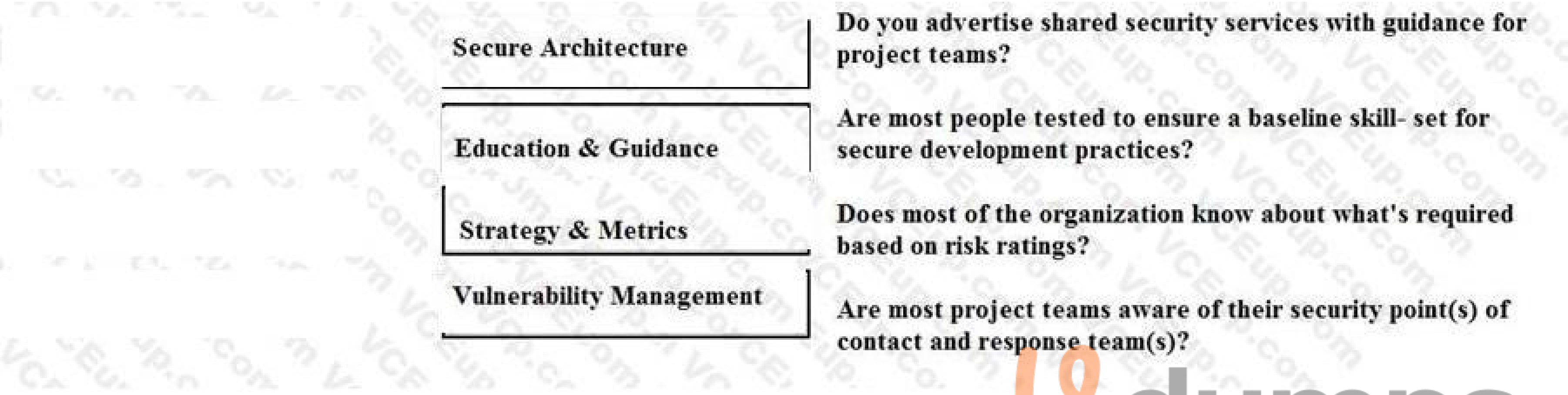
Do you advertise shared security services with guidance for project teams?

Are most people tested to ensure a baseline skill- set for secure development practices?

Does most of the organization know about what's required based on risk ratings?

Are most project teams aware of their security point(s) of contact and response team(s)?

Correct Answer:

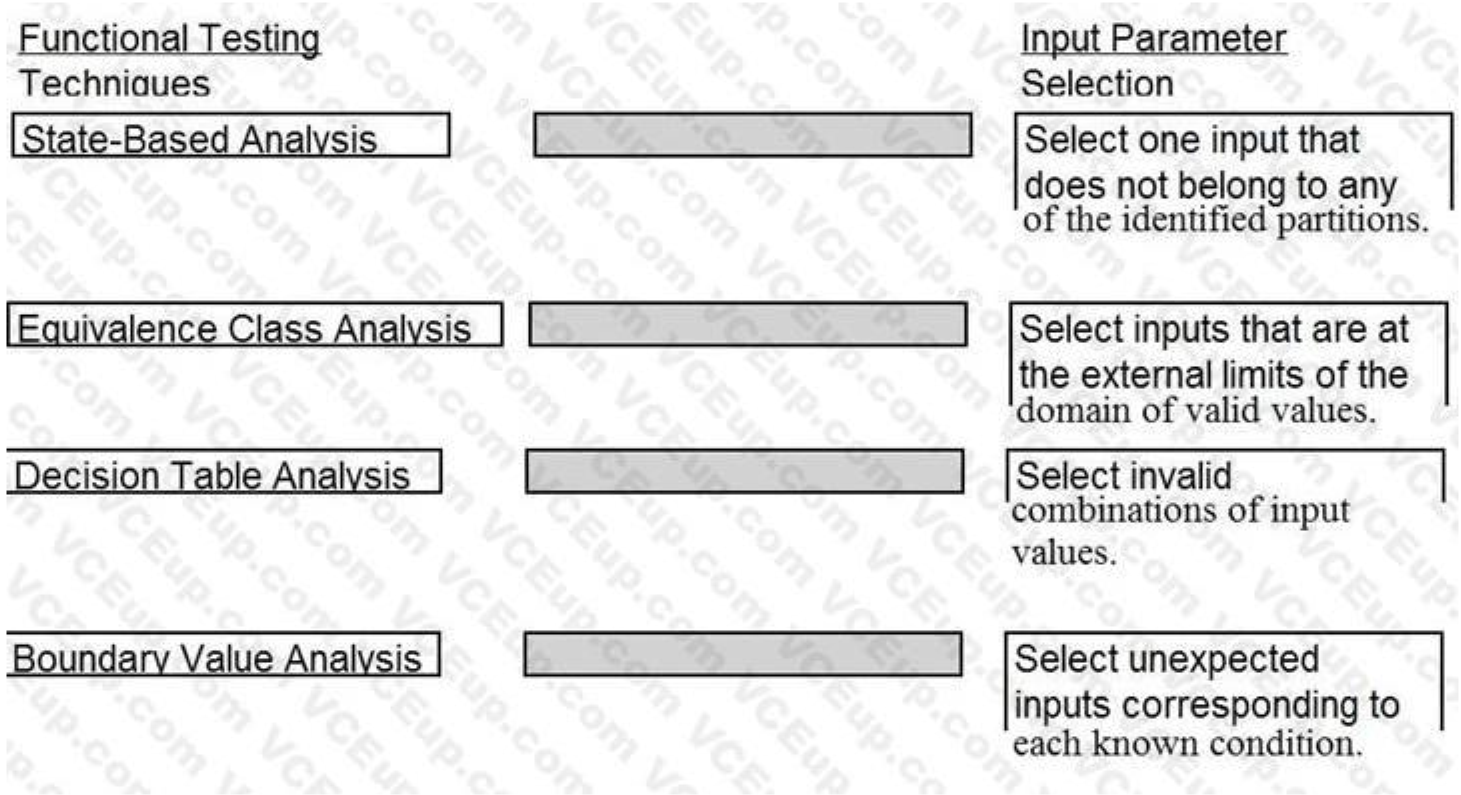


Secure Architecture	Do you advertise shared security services with guidance for project teams?
Education & Guidance	Are most people tested to ensure a baseline skill- set for secure development practices?
Strategy & Metrics	Does most of the organization know about what's required based on risk ratings?
Vulnerability Management	Are most project teams aware of their security point(s) of contact and response team(s)?

Section:
Explanation:

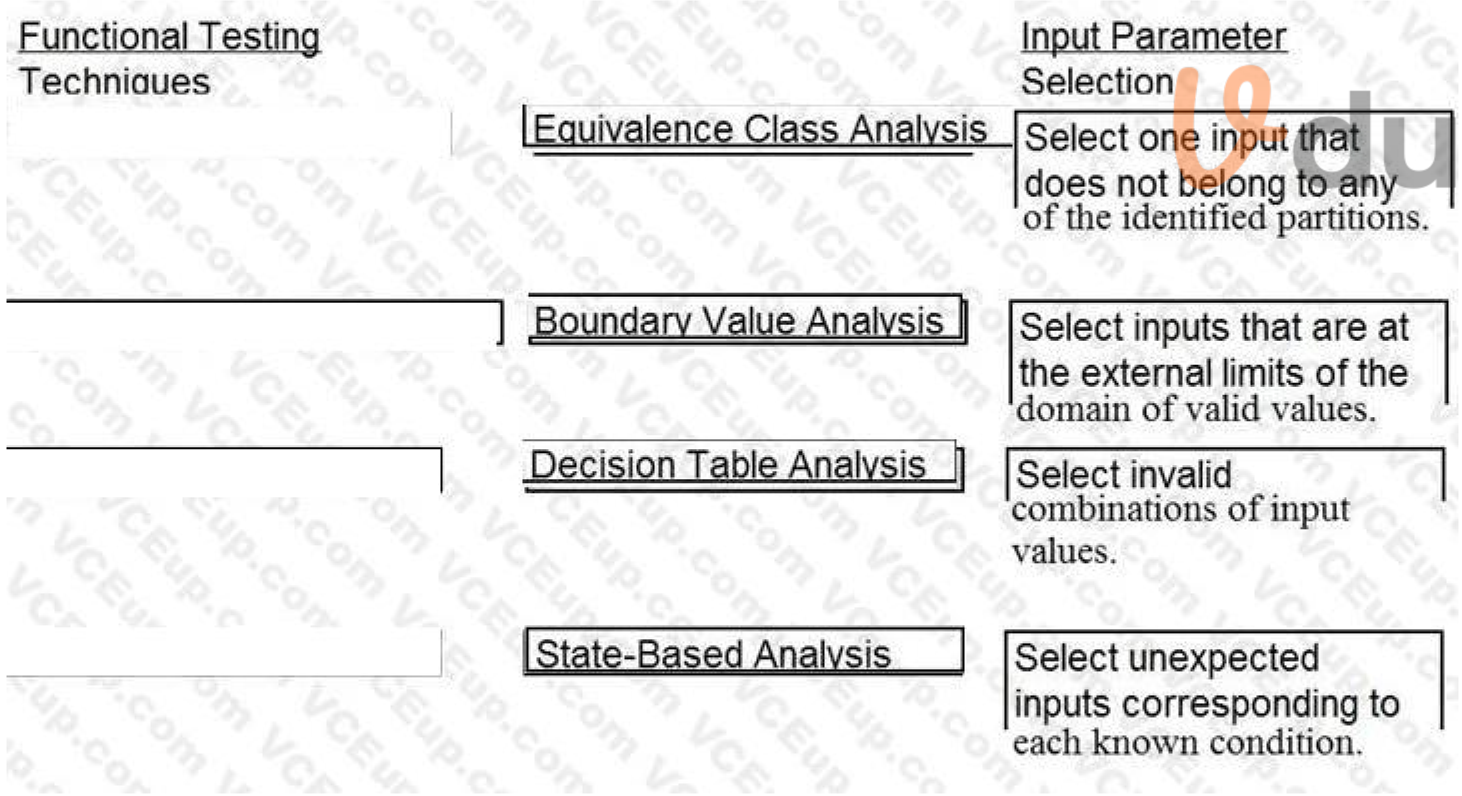
QUESTION 490
DRAG DROP
A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

Select and Place:



Functional Testing Techniques		Input Parameter Selection
State-Based Analysis		Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis		Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis		Select invalid combinations of input values.
Boundary Value Analysis		Select unexpected inputs corresponding to each known condition.

Correct Answer:

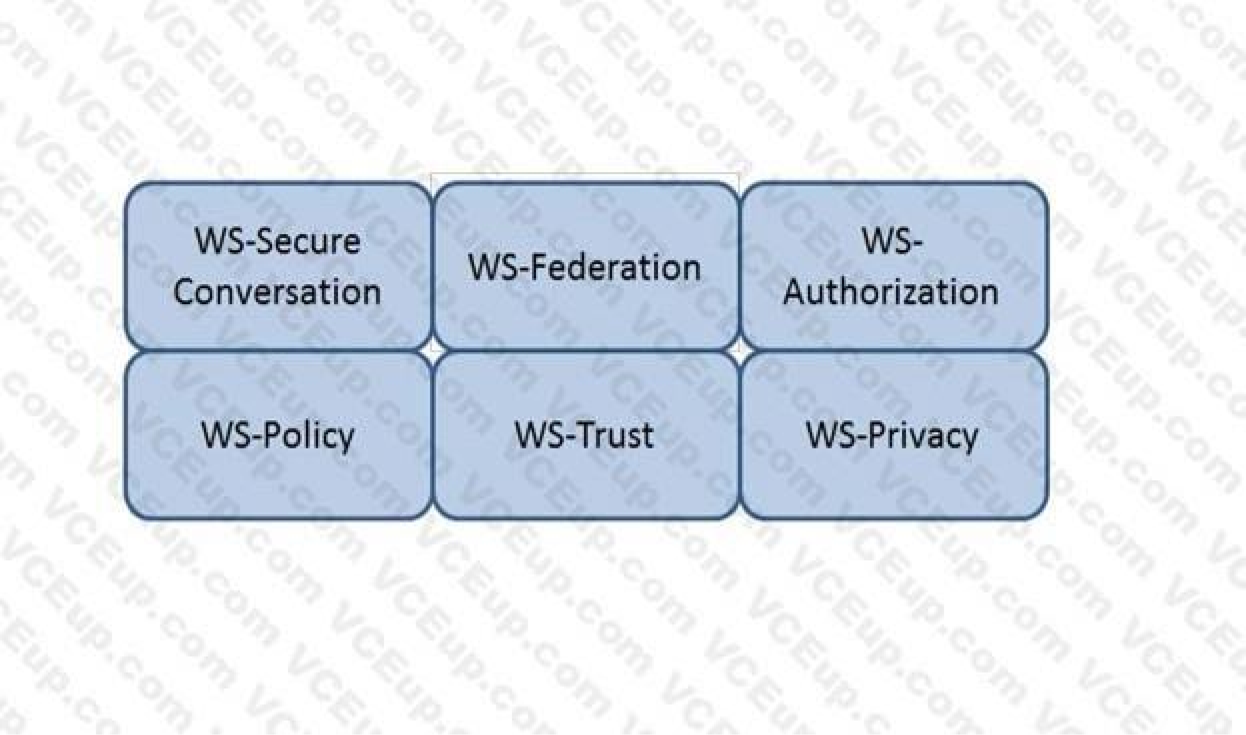


Functional Testing Techniques		Input Parameter Selection
	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
	Decision Table Analysis	Select invalid combinations of input values.
	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

Section:
Explanation:

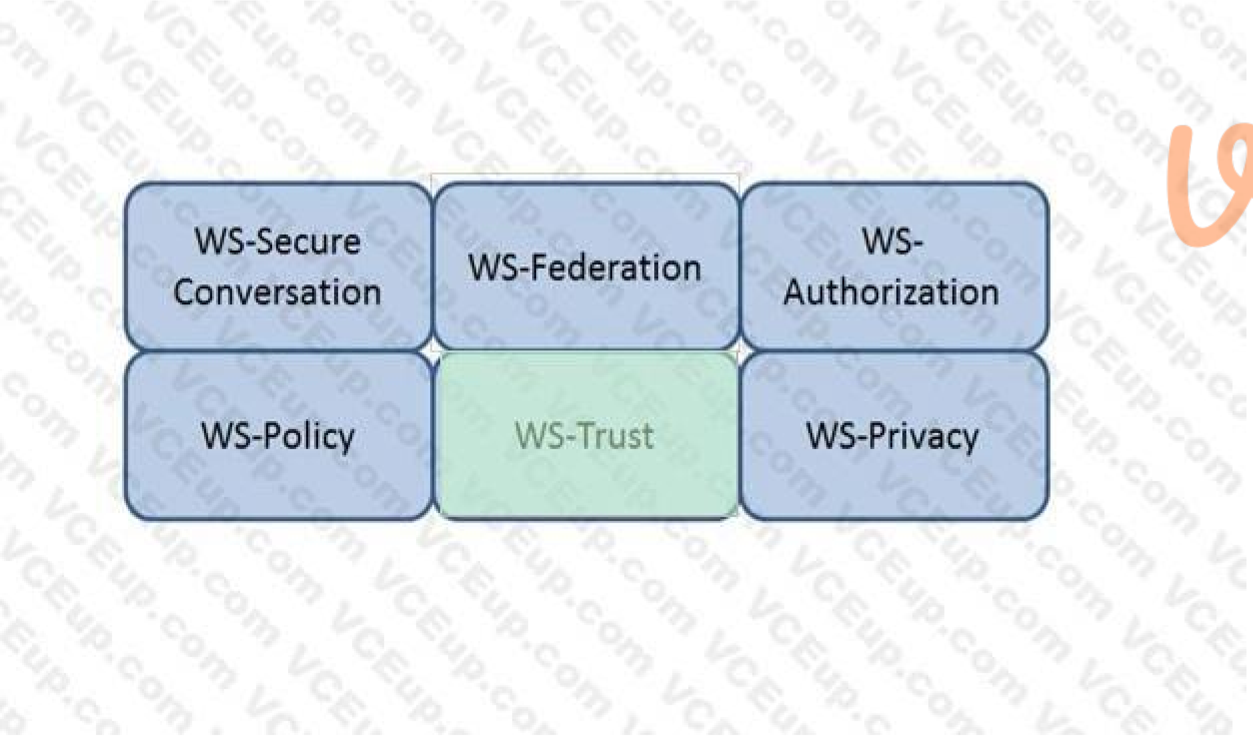
QUESTION 491
HOTSPOT
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.

Hot Area:



WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

Answer Area:

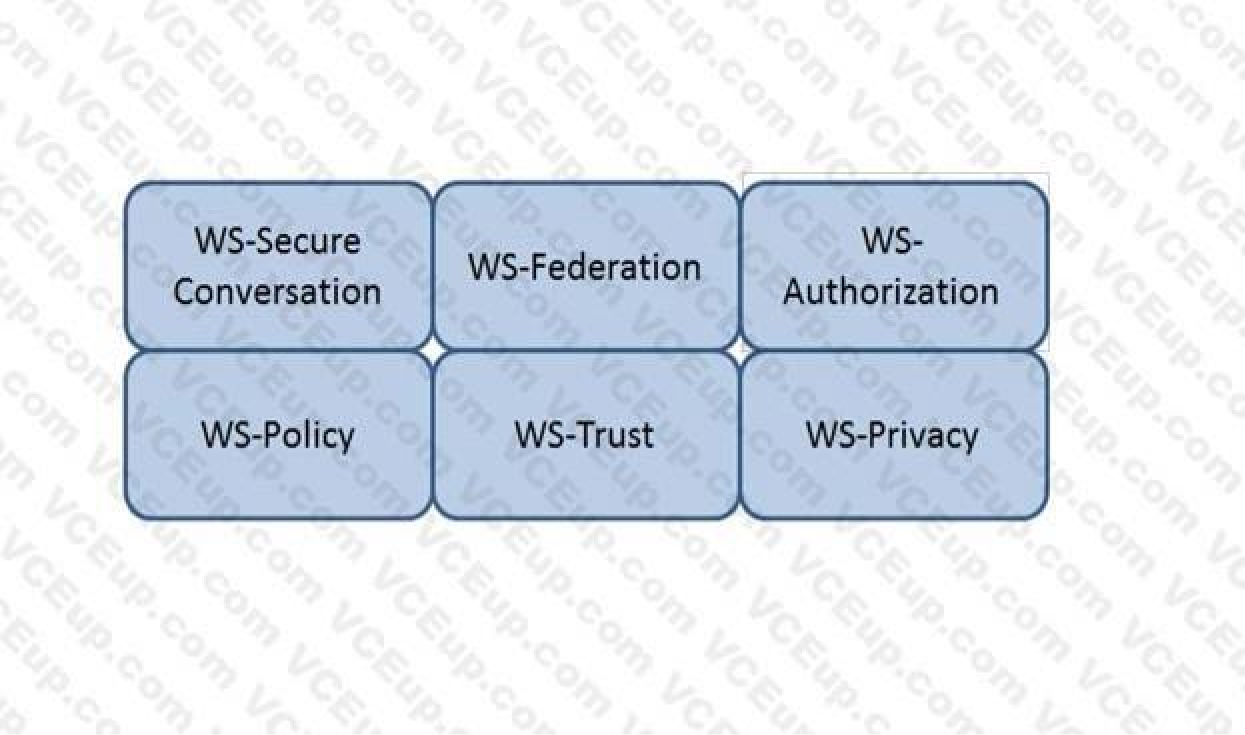


WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

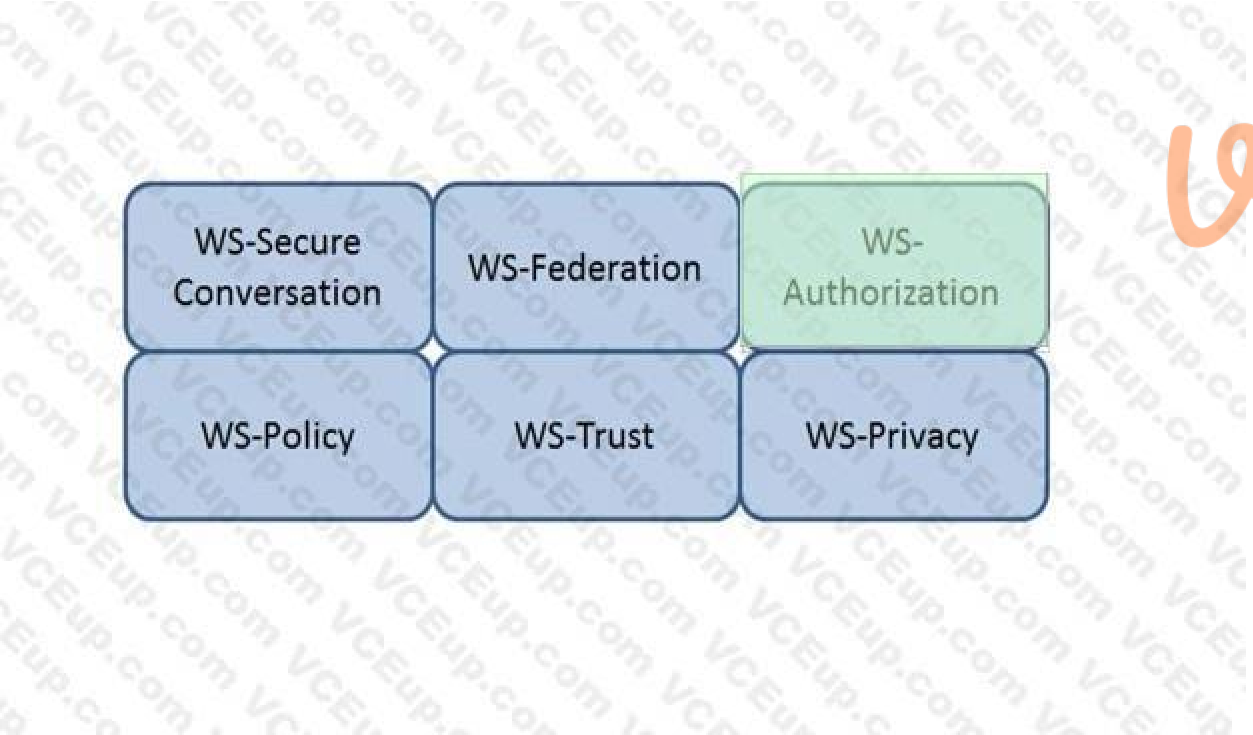
Section:
Explanation:
WS-Federation
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

QUESTION 492
HOTSPOT
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.

Hot Area:



Answer Area:



Section:
Explanation:

QUESTION 493
Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management's directive?

A. Strict integration of application management, configuration management (CM), and phone management
B. Management application installed on user phones that tracks all application events and cellular traffic
C. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity

D. Routine reports generated by the user's cellular phone provider that detail security events

Correct Answer: B
Section:

QUESTION 494
What is the FIRST step prior to executing a test of an organisation's disaster recovery (DR) or business continuity plan (BCP)?

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

Correct Answer: D
Section:

QUESTION 495
Which of the following security tools will ensure authorized data is sent to the application when implementing a cloud based application?

A. Host-based intrusion prevention system (HIPS)
B. Access control list (ACL)
C. File integrity monitoring (FIM)
D. Data loss prevention (DLP)

Correct Answer: B
Section:

QUESTION 496
Before implementing an internet-facing router, a network administrator ensures that the equipment is baselined/hardened according to approved configurations and settings. This action provides protection against which of the following attacks?

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

Correct Answer: B
Section:

QUESTION 497
A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging generates extremely high amount of logs.
What is the MOST appropriate strategy for the log retention?

A. Keep last week's logs in an online storage and the rest in a near-line storage.
B. Keep all logs in an online storage.
C. Keep all logs in an offline storage.

D. Keep last week's logs in an online storage and the rest in an offline storage.

Correct Answer: D
Section:

QUESTION 498
Which of the following is the MOST comprehensive Business Continuity (BC) test?

A. Full functional drill
B. Full table top
C. Full simulation
D. Full interruption

Correct Answer: C
Section:

QUESTION 499
The disaster recovery (DR) process should always include

A. plan maintenance.
B. periodic vendor review.
C. financial data analysis.
D. periodic inventory review.

Correct Answer: A
Section:

QUESTION 500
Which of the following BEST describes the purpose of software forensics?

A. To perform cyclic redundancy check (CRC) verification and detect changed applications
B. To review program code to determine the existence of backdoors
C. To analyze possible malicious intent of malware
D. To determine the author and behavior of the code

Correct Answer: D
Section:

QUESTION 501
The security architect has been assigned the responsibility of ensuring integrity of the organization's electronic records. Which of the following methods provides the strongest level of integrity?

A. Time stamping
B. Encryption
C. Hashing
D. Digital signature

Correct Answer: D

Section:

QUESTION 502
An application is used for funds transfer between an organization and a third-party. During a security audit, an issue with the business continuity/disaster recovery policy and procedures for this application. Which of the following reports should the audit file with the organization?

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

Correct Answer: C
Section:

QUESTION 503
An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weal

A. Implement a dedicated COTS sandbox environment
B. Follow the software end-of-life schedule
C. Transfer the risk to the cloud service provider
D. Examine the software updating and patching process

Correct Answer: A
Section:

QUESTION 504
Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users internal control over financial reporting?

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

Correct Answer: B
Section:

QUESTION 505
The Chief Information Security Officer (CISO) is concerned about business application availability. The organization was recently subject to a ransomware attack that resulted in the unavailability of applications and services for 10 working days that required paper-based running of all main business processes. There are now aggressive plans to enhance the Recovery Time Objective (RTO) and cater for more frequent data captures. Which of the following solutions should be implemented to fully comply to the new business requirements?

A. Virtualization
B. Antivirus
C. Process isolation
D. Host-based intrusion prevention system (HIPS)

Correct Answer: A
Section:

QUESTION 506
Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

A. Organizations can only reach a maturity level 3 when using CMMs
B. CMMs do not explicitly address safety and security
C. CMMs can only be used for software developed in-house
D. CMMs are vendor specific and may be biased

Correct Answer: B
Section:

QUESTION 507
Which of the following should exist in order to perform a security audit?

A. Industry framework to audit against
B. External (third-party) auditor
C. Internal certified auditor
D. Neutrality of the auditor

Correct Answer: D
Section:

QUESTION 508
Which of the following encryption technologies has the ability to function as a stream cipher?

A. Cipher Feedback (CFB)
B. Feistel cipher
C. Cipher Block Chaining (CBC) with error propagation
D. Electronic Code Book (ECB)

Correct Answer: A
Section:

QUESTION 509
An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of which of the following types of attack?

A. Cross-Site Scripting (XSS)
B. Cross-site request forgery (CSRF)
C. Injection
D. Click jacking

Correct Answer: B
Section:

QUESTION 510
Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

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

Correct Answer: A
Section:

QUESTION 511
A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

A. Remove the ultraviolet light filters on the HVAC intake and replace the fire suppression system on the upper floors with a dry system
B. Add additional ultraviolet light filters to the HVAC intake supply and return ducts and change server room fire suppression to FM-200
C. Apply additional physical security around the HVAC intakes and update upper floor fire suppression to FM-200.
D. Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system

Correct Answer: C
Section:

QUESTION 512
An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is
MOST effective for the SMP?

A. Data driven risk assessment with a focus on data
B. Security controls driven assessment that focuses on controls management
C. Business processes based risk assessment with a focus on business goals
D. Asset driven risk assessment with a focus on the assets

Correct Answer: A
Section:

QUESTION 513
Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

A. Diffie-hellman (DH) key exchange: DH (>=2048 bits)
Symmetric Key: Advanced Encryption Standard (AES) > 128 bits
Digital Signature: Rivest-Shamir-Adleman (RSA) (1024 bits)
B. Diffie-hellman (DH) key exchange: DH (>=2048 bits)
Symmetric Key: Advanced Encryption Standard (AES) > 128 bits
Digital Signature: Digital Signature Algorithm (DSA) (>=2048 bits)
C. Diffie-hellman (DH) key exchange: DH (<= 1024 bits)

Symmetric Key: Blowfish
Digital Signature: Rivest-Shamir-Adleman (RSA) (>=2048 bits)

D. Diffie-hellman (DH) key exchange: DH (>=2048 bits)
Symmetric Key: Advanced Encryption Standard (AES) < 128 bits
Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) (>=256 bits)

Correct Answer: C
Section:

QUESTION 514

An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP), The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract.
Which of the following MUST be included in the contract?

A. A detailed overview of all equipment involved in the outsourcing contract
B. The MSSP having an executive manager responsible for information security
C. The right to perform security compliance tests on the MSSP's equipment
D. The right to audit the MSSP's security process

Correct Answer: C
Section:

QUESTION 515

Which of the following is the MOST effective measure for dealing with rootkit attacks?

A. Turing off unauthorized services and rebooting the system
B. Finding and replacing the altered binaries with legitimate ones
C. Restoring the system from the last backup
D. Reinstalling the system from trusted sources

Correct Answer: D
Section:

QUESTION 516

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

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

Correct Answer: C
Section:

QUESTION 517

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

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

Correct Answer: A
Section:

QUESTION 518
What is the MOST important factor in establishing an effective Information Security Awareness Program?

A. Obtain management buy-in.
B. Conduct an annual security awareness event.
C. Mandate security training.
D. Hang information security posters on the walls,

Correct Answer: C
Section:

QUESTION 519
Which of the following events prompts a review of the disaster recovery plan (DRP)?

A. New members added to the steering committee
B. Completion of the security policy review
C. Change in senior management
D. Organizational merger

Correct Answer: D
Section:

QUESTION 520
An organization plans to acquire @ commercial off-the-shelf (COTS) system to replace their aging home-built reporting system. When should the organization's security team FIRST get involved in this acquisition's life cycle?

A. When the system is being designed, purchased, programmed, developed, or otherwise constructed
B. When the system is verified and validated
C. When the system is deployed into production
D. When the need for a system is expressed and the purpose of the system Is documented

Correct Answer: D
Section:

QUESTION 521
A developer begins employment with an information technology (IT) organization. On the first day, the developer works through the list of assigned projects and finds that some files within those projects aren't accessible, Other developers working on the same project have no trouble locating and working on the. What is the MOST likely for the discrepancy in access?

A. The IT administrator had failed to grant the developer privileged access to the servers.
B. The project files were inadvertently deleted.

C. The new developer's computer had not been added to an access control list (ACL).
D. The new developer's user account was not associated with the right roles needed for the projects.

Correct Answer: A
Section:

QUESTION 522
Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

A. Review applicable destination country laws, forensically clean devices prior to travel, and only download sensitive data over a virtual private network (VPN) upon arriving at the destination.
B. Keep laptops, external storage devices, and smartphones in the hotel room when not in use.
C. Leverage a Secure Socket Layer (SSL) connection over a virtual private network (VPN) to download sensitive data upon arriving at the destination.
D. Use multi-factor authentication (MFA) to gain access to data stored on laptops or external storage devices and biometric fingerprint access control isms to unlock smartphones.

Correct Answer: D
Section:

QUESTION 523
Which of the following implementations will achieve high availability in a website?

A. Multiple Domain Name System (DNS) entries resolving to the same web server and large amounts of bandwidth
B. Disk mirroring of the web server with redundant disk drives in a hardened data center
C. Disk striping of the web server hard drives and large amounts of bandwidth
D. Multiple geographically dispersed web servers that are configured for failover

Correct Answer: D
Section:

QUESTION 524
Which of the following phases in the software acquisition process does developing evaluation criteria take place?

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

Correct Answer: D
Section:

QUESTION 525
Security Software Development Life Cycle (SDLC) expects application code to be written In a consistent manner to allow ease of auditing and which of the following?

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

Correct Answer: A
Section:

QUESTION 526
In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

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

Correct Answer: C
Section:

QUESTION 527
Which of the following is considered the FIRST step when designing an internal security control assessment?

A. Create a plan based on recent vulnerability scans of the systems in question.
B. Create a plan based on comprehensive knowledge of known breaches.
C. Create a plan based on a recognized framework of known controls.
D. Create a plan based on reconnaissance of the organization's infrastructure.

Correct Answer: D
Section:

QUESTION 528
The Chief Executive Officer (CEO) wants to implement an internal audit of the company's information security posture. The CEO wants to avoid any bias in the audit process; therefore, has assigned the Sales Director to conduct the audit.
After significant interaction over a period of weeks the audit concludes that the company's policies and procedures are sufficient, robust and well established. The CEO then moves on to engage an external penetration testing company in order to showcase the organization's robust information security stance. This exercise reveals significant failings in several critical security controls and shows that the incident response processes remain undocumented.
What is the MOST likely reason for this disparity in the results of the audit and the external penetration test?

A. The external penetration testing company used custom zero-day attacks that could not have been predicted.
B. The information technology (IT) and governance teams have failed to disclose relevant information to the internal audit team leading to an incomplete assessment being formulated.
C. The scope of the penetration test exercise and the internal audit were significantly different.
D. The audit team lacked the technical experience and training to make insightful and objective assessments of the data provided to them.

Correct Answer: C
Section:

QUESTION 529
A small office is running WiFi 4 APs, and neighboring offices do not want to increase the throughput to associated devices. Which of the following is the MOST cost-efficient way for the office to increase network performance?

A. Add another AP.
B. Disable the 2.4GHz radios

C. Enable channel bonding.
D. Upgrade to WiFi 5.

Correct Answer: C
Section:

QUESTION 530
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

A. The link is improperly terminated
B. One of the devices is misconfigured
C. The cable length is excessive.
D. One of the devices has a hardware issue.

Correct Answer: A
Section:

QUESTION 531
Which of the following VPN configurations should be used to separate Internet and corporate traffic?

A. Split-tunnel
B. Remote desktop gateway
C. Site-to-site
D. Out-of-band management

Correct Answer: A
Section:

QUESTION 532
A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

A. Omni
B. Directional
C. Yagi
D. Parabolic

Correct Answer: A
Section:

QUESTION 533
To comply with industry requirements, a security assessment on the cloud server should identify which protocols and weaknesses are being exposed to attackers on the Internet. Which of the following tools is the MOST appropriate to complete the assessment?

A. Use tcpdump and parse the output file in a protocol analyzer.
B. Use an IP scanner and target the cloud WAN network addressing
C. Run netstat in each cloud server and retrieve the running processes.
D. Use nmap and set the servers' public IPs as the targets.

Correct Answer: D
Section:

QUESTION 534
Which of the following uses the destination IP address to forward packets?

A. A bridge
B. A Layer 2 switch
C. A router
D. A repeater

Correct Answer: C
Section:

QUESTION 535
Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

A. Scope options
B. Reservation
C. Dynamic assignment
D. Exclusion
E. Static assignment

Correct Answer: B
Section:

QUESTION 536
Wireless users are reporting intermittent Internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time. The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client's wireless settings.
C. Confirm that a valid passphrase is being used during the web authentication.
D. Investigate for a client's disassociation caused by an evil twin AP

Correct Answer: A
Section:

QUESTION 537
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

A. OTDR
B. Tone generator
C. Fusion splicer
D. Cable tester
E. PoE injector

Correct Answer: A
Section:

QUESTION 538
Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

A. Client-to-site VPN
B. Third-party VPN service
C. Site-to-site VPN
D. Split-tunnel VPN

Correct Answer: C
Section:

QUESTION 539
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch.
Which of the following command-line tools should the technician use to determine where the incident is occurring?

A. nslookup
B. show config
C. netstat
D. show interface
E. show counters

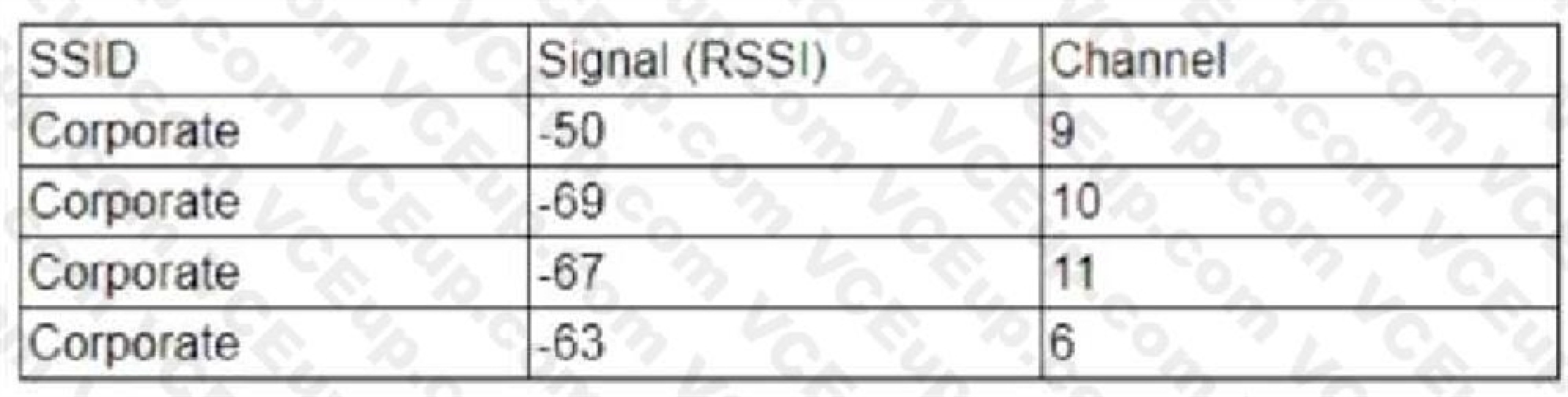
Correct Answer: D
Section:

QUESTION 540
Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

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

Correct Answer: C
Section:

QUESTION 541
A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:



SSID	Signal (RSSI)	Channel
Corporate	-50	9
Corporate	-69	10
Corporate	-67	11
Corporate	-63	6

Which of the following is MOST likely the cause of the issue?

A. Channel overlap
B. Poor signal
C. Incorrect power settings
D. Wrong antenna type

Correct Answer: A
Section:

QUESTION 542
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

A. Layer 3 switch
B. VPN headend
C. Next-generation firewall
D. Proxy server
E. Intrusion prevention

Correct Answer: C
Section:

QUESTION 543
A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

A. Virtual network computing
B. Secure Socket Shell
C. in-band connection
D. Site-to-site VPN

Correct Answer: D
Section: