



ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1

- (Exam Topic 15)

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

Answer: D

NEW QUESTION 2

- (Exam Topic 15)

An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

- A. Deduplication
- B. Compression
- C. Replication
- D. Caching

Answer: B

NEW QUESTION 3

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 4

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 5

- (Exam Topic 15)

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

Answer: A

NEW QUESTION 6

- (Exam Topic 15)

Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless

Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

- A. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network bridge in order to communicate.
- B. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network bridge in order to communicate.
- C. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network router in order to communicate.
- D. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network router in order to communicate.

Answer: B

NEW QUESTION 7

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 8

- (Exam Topic 15)

he security organization is loading for a solution that could help them determine with a strong level of confident that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

- A. Installing an intrusion prevention system (IPS)
- B. Deploying a honeypot
- C. Installing an intrusion detection system (IDS)
- D. Developing a sandbox

Answer: B

NEW QUESTION 9

- (Exam Topic 15)

Which of the following access control models is MOST restrictive?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 15)

Which of the following is established to collect information Se eee ee ee nation readily available in part through implemented security controls?

- A. Security Assessment Report (SAR)
- B. Organizational risk tolerance
- C. Information Security Continuous Monitoring (ISCM)
- D. Risk assessment report

Answer: D

NEW QUESTION 10

- (Exam Topic 15)

Which of the following is a PRIMARY security weakness in the design of Domain Name System (DNS)?

- A. A DNS server can be disabled in a denial-of-service (DoS) attack.
- B. A DNS server does not authenticate source of information.
- C. Each DNS server must hold the address of the root servers.
- D. A DNS server database can be injected with falsified checksums.

Answer: A

NEW QUESTION 11

- (Exam Topic 15)

A breach investigation a website was exploited through an open sourcedIs The FIRB Stan In the Process that could have prevented this breach?

- A. Application whitelisting
- B. Web application firewall (WAF)
- C. Vulnerability remediation
- D. Software inventory

Answer: B

NEW QUESTION 13

- (Exam Topic 15)

A cybersecurity engineer has been tasked to research and implement an ultra-secure communications channel to protect the organization's most valuable intellectual property (IP). The primary directive in this initiative is to ensure there Is no possible way the communications can be intercepted without detection. Which of the following Is the only way to ensure this 'outcome'?

- A. Diffie-Hellman key exchange
- B. Symmetric key cryptography
- C. [Public key infrastructure (PKI)
- D. Quantum Key Distribution

Answer: C

NEW QUESTION 16

- (Exam Topic 15)

When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

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

Answer: C

NEW QUESTION 18

- (Exam Topic 15)

When reviewing the security logs, the password shown for an administrative login event was ' OR '1'=1' --. This is an example of which of the following kinds of attack?

- A. Brute Force Attack
- B. Structured Query Language (SQL) Injection
- C. Cross-Site Scripting (XSS)
- D. Rainbow Table Attack

Answer: B

NEW QUESTION 20

- (Exam Topic 15)

A company is moving from the V model to Agile development. How can the information security department BEST ensure that secure design principles are implemented in the new methodology?

- A. All developers receive a mandatory targeted information security training.
- B. The non-financial information security requirements remain mandatory for the new model.
- C. The information security department performs an information security assessment after each sprint.
- D. Information security requirements are captured in mandatory user stories.

Answer: D

NEW QUESTION 24

- (Exam Topic 15)

In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to the resource's access to the production operating system (OS) directory structure?

- A. From Read Only privileges to No Access Privileges
- B. From Author privileges to Administrator privileges
- C. From Administrator privileges to No Access privileges
- D. From No Access Privileges to Author privileges

Answer: C

NEW QUESTION 27

- (Exam Topic 15)

Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

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

Answer: D

NEW QUESTION 32

- (Exam Topic 15)

An attacker is able to remain indefinitely logged into a exploiting to remain on the web service?

- A. Alert management
- B. Password management
- C. Session management
- D. Identity management (IM)

Answer: C

NEW QUESTION 37

- (Exam Topic 15)

What is the FIRST step for an organization to take before allowing personnel to access social media from a corporate device or user account?

- A. Publish a social media guidelines document.
- B. Publish an acceptable usage policy.
- C. Document a procedure for accessing social media sites.

D. Deliver security awareness training.

Answer: A

NEW QUESTION 39

- (Exam Topic 15)

A security practitioner has been asked to model best practices for disaster recovery (DR) and business continuity. The practitioner has decided that a formal committee is needed to establish a business continuity policy. Which of the following BEST describes this stage of business continuity development?

- A. Project Initiation and Management
- B. Risk Evaluation and Control
- C. Developing and Implementing business continuity plans (BCP)
- D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 41

- (Exam Topic 15)

Which access control method is based on users issuing access requests on system resources, features assigned to those resources, the operational or situational context, and a set of policies specified in terms of those features and context?

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

Answer: B

NEW QUESTION 42

- (Exam Topic 15)

A software developer installs a game on their organization-provided smartphone. Upon installing the game, the software developer is prompted to allow the game access to call logs, Short Message Service (SMS) messaging, and Global Positioning System (GPS) location data. What has the game MOST likely introduced to the smartphone?

- A. Alerting
- B. Vulnerability
- C. Geo-fencing
- D. Monitoring

Answer: B

NEW QUESTION 47

- (Exam Topic 15)

A project manager for a large software firm has acquired a government contract that generates large amounts of Controlled Unclassified Information (CUI). The organization's information security manager has received a request to transfer project-related CUI between systems of differing security classifications. What role provides the authoritative guidance for this transfer?

- A. Information owner
- B. PM
- C. Data Custodian
- D. Mission/Business Owner

Answer: C

NEW QUESTION 49

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 54

- (Exam Topic 15)

What type of investigation applies when malicious behavior is suspected between two organizations?

- A. Regulatory
- B. Criminal
- C. Civil
- D. Operational

Answer: A

NEW QUESTION 57

- (Exam Topic 15)

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

Answer: A

NEW QUESTION 60

- (Exam Topic 15)

Physical Access Control Systems (PACS) allow authorized security personnel to manage and monitor access control for subjects through which function?

- A. Remote access administration
- B. Personal Identity Verification (PIV)
- C. Access Control List (ACL)
- D. Privileged Identity Management (PIM)

Answer: B

NEW QUESTION 61

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 64

- (Exam Topic 15)

What is the MOST effective response to a hacker who has already gained access to a network and will attempt to pivot to other resources?

- A. Reset all passwords.
- B. Shut down the network.
- C. Warn users of a breach.
- D. Segment the network.

Answer: D

NEW QUESTION 68

- (Exam Topic 15)

Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

- A. Data at rest has been compromised when the user has authenticated to the device.
- B. Data on the device cannot be restored from backup.
- C. Data in transit has been compromised when the user has authenticated to the device.
- D. Data on the device cannot be backed up.

Answer: A

NEW QUESTION 71

- (Exam Topic 15)

Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

- A. Directory
- B. User database
- C. Multi-factor authentication (MFA)
- D. Single sign-on (SSO)

Answer: A

NEW QUESTION 72

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 75

- (Exam Topic 15)

Using the cipher text and resultant clear text message to derive the non-alphabetic cipher key is an example of which method of cryptanalytic attack?

- A. Frequency analysis
- B. Ciphertext-only attack
- C. Probable-plaintext attack
- D. Known-plaintext attack

Answer: D

NEW QUESTION 78

- (Exam Topic 15)

What is the term used to define where data is geographically stored in the cloud?

- A. Data warehouse
- B. Data privacy rights
- C. Data subject rights
- D. Data sovereignty

Answer: D

NEW QUESTION 80

- (Exam Topic 15)

Which of the following is included in change management?

- A. Business continuity testing
- B. User Acceptance Testing (UAT) before implementation
- C. Technical review by business owner
- D. Cost-benefit analysis (CBA) after implementation

Answer: A

NEW QUESTION 85

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 86

- (Exam Topic 15)

Which of the following is MOST important to follow when developing information security controls for an organization?

- A. Exercise due diligence with regard to all risk management information to tailor appropriate controls.
- B. Perform a risk assessment and choose a standard that addresses existing gaps.
- C. Use industry standard best practices for security controls in the organization.
- D. Review all local and international standards and choose the most stringent based on location.

Answer: C

NEW QUESTION 89

- (Exam Topic 15)

Which of the following addresses requirements of security assessment during software acquisition?

- A. Software assurance policy
- B. Continuous monitoring
- C. Software configuration management (SCM)
- D. Data loss prevention (DLP) policy

Answer: B

NEW QUESTION 92

- (Exam Topic 15)

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

Answer: A

NEW QUESTION 94

- (Exam Topic 15)

When testing password strength, which of the following is the BEST method for brute forcing passwords?

- A. Conduct an offline attack on the hashed password information.
- B. Conduct an online password attack until the account being used is locked.
- C. Use a comprehensive list of words to attempt to guess the password.
- D. Use social engineering methods to attempt to obtain the password.

Answer: C

NEW QUESTION 98

- (Exam Topic 15)

A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

- A. Hybrid frequency band, service set identifier (SSID), and interpolation
- B. Performance, geographic location, and radio signal interference
- C. Facility size, intermodulation, and direct satellite service
- D. Existing client devices, manufacturer reputation, and electrical interference

Answer: D

NEW QUESTION 101

- (Exam Topic 15)

A client server infrastructure that provides user-to-server authentication describes which one of the following?

- A. Secure Sockets Layer (SSL)
- B. Kerberos
- C. 509
- D. User-based authorization

Answer: B

NEW QUESTION 103

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 107

- (Exam Topic 15)

Which of the following determines how traffic should flow based on the status of the infrastructure layer?

- A. Traffic plane
- B. Application plane
- C. Data plane
- D. Control plane

Answer: A

NEW QUESTION 112

- (Exam Topic 15)

Which of the following are the BEST characteristics of security metrics?

- A. They are generalized and provide a broad overview
- B. They use acronyms and abbreviations to be concise
- C. They use bar charts and Venn diagrams
- D. They are consistently measured and quantitatively expressed

Answer: D

NEW QUESTION 115

- (Exam Topic 15)

Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

- A. Transport Layer
- B. Data Link and Physical Layers
- C. Application, Presentation, and Session Layers
- D. Session and Network Layers

Answer: B

NEW QUESTION 119

- (Exam Topic 15)

What security principle addresses the issue of "Security by Obscurity"?

- A. Open design
- B. Segregation of duties (SoD)
- C. Role Based Access Control (RBAC)
- D. Least privilege

Answer: D

NEW QUESTION 124

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 129

- (Exam Topic 15)

Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

- A. Data emanation, deploying Category (CAT) 6 and higher cable wherever feasible
- B. Light leakage, deploying shielded cable wherever feasible
- C. Cable damage, deploying ring architecture wherever feasible
- D. Electronic eavesdropping, deploying end-to-end encryption wherever feasible

Answer: B

NEW QUESTION 131

- (Exam Topic 15)

Computer forensics requires which of the following MAIN steps?

- A. Announce the incident to responsible sections, analyze the data, assimilate the data for correlation
- B. Take action to contain the damage, announce the incident to responsible sections, analyze the data
- C. Acquire the data without altering, authenticate the recovered data, analyze the data
- D. Access the data before destruction, assimilate the data for correlation, take action to contain the damage

Answer: B

NEW QUESTION 134

- (Exam Topic 15)

Which of the following is the MOST appropriate control for asset data labeling procedures?

- A. Logging data media to provide a physical inventory control
- B. Reviewing audit trails of logging records
- C. Categorizing the types of media being used
- D. Reviewing off-site storage access controls

Answer: C

NEW QUESTION 137

- (Exam Topic 15)

An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

- A. RAID level 1

- B. RAID level 3
- C. RAID level 4
- D. RAID level 5

Answer: D

NEW QUESTION 139

- (Exam Topic 15)

Which of the following departments initiates the request, approval, and provisioning business process?

- A. Operations
- B. Human resources (HR)
- C. Information technology (IT)
- D. Security

Answer: A

NEW QUESTION 140

- (Exam Topic 15)

Which one of the following BEST protects vendor accounts that are used for emergency maintenance?

- A. Encryption of routing tables
- B. Vendor access should be disabled until needed
- C. Role-based access control (RBAC)
- D. Frequent monitoring of vendor access

Answer: B

NEW QUESTION 142

- (Exam Topic 15)

Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

- A. A network-based firewall is stateful, while a host-based firewall is stateless.
- B. A network-based firewall controls traffic passing through the device, while a host-based firewall controls traffic destined for the device.
- C. A network-based firewall verifies network traffic, while a host-based firewall verifies processes and applications.
- D. A network-based firewall blocks network intrusions, while a host-based firewall blocks malware.

Answer: B

NEW QUESTION 145

- (Exam Topic 15)

Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

- A. Cutover
- B. Walkthrough
- C. Tabletop
- D. Parallel

Answer: C

NEW QUESTION 149

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 153

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 156

- (Exam Topic 15)

In systems security engineering, what does the security principle of modularity provide?

- A. Documentation of functions
- B. Isolated functions and data
- C. Secure distribution of programs and data
- D. Minimal access to perform a function

Answer: A

NEW QUESTION 158

- (Exam Topic 15)

When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

- A. Annual Loss Expectancy (ALE) + Work Recovery Time (WRT)
- B. Business impact analysis (BIA) + Recovery Point Objective (RPO)
- C. Recovery Time Objective (RTO) + Work Recovery Time (WRT)
- D. Estimated Maximum Loss (EML) + Recovery Time Objective (RTO)

Answer: C

NEW QUESTION 163

- (Exam Topic 15)

When assessing the audit capability of an application, which of the following activities is MOST important?

- A. Determine if audit records contain sufficient information.
- B. Review security plan for actions to be taken in the event of audit failure.
- C. Verify if sufficient storage is allocated for audit records.
- D. Identify procedures to investigate suspicious activity.

Answer: C

NEW QUESTION 165

- (Exam Topic 15)

After the INITIAL input of a user identification (ID) and password, what is an authentication system that prompts the user for a different response each time the user logs on?

- A. Persons Identification Number (PIN)
- B. Secondary password
- C. Challenge response
- D. Voice authentication

Answer: C

NEW QUESTION 168

- (Exam Topic 15)

A security professional has been assigned to assess a web application. The assessment report recommends switching to Security Assertion Markup Language (SAML). What is the PRIMARY security benefit in switching to SAML?

- A. It uses Transport Layer Security (TLS) to address confidentiality.
- B. it enables single sign-on (SSO) for web applications.
- C. The users' password is not passed during authentication.
- D. It limits unnecessary data entry on web forms.

Answer: B

NEW QUESTION 170

- (Exam Topic 15)

What BEST describes the confidentiality, integrity, availability triad?

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

Answer: C

NEW QUESTION 174

- (Exam Topic 15)

Which of the following security tools monitors devices and records the information in a central database for further analysis?

- A. Security orchestration automation and response
- B. Host-based intrusion detection system (HIDS)
- C. Antivirus
- D. Endpoint detection and response (EDR)

Answer: A

NEW QUESTION 177

- (Exam Topic 15)

What is the FINAL step in the waterfall method for contingency planning?

- A. Maintenance
- B. Testing
- C. Implementation
- D. Training

Answer: A

NEW QUESTION 182

- (Exam Topic 15)

Commercial off-the-shelf (COTS) software presents which of the following additional security concerns?

- A. Vendors take on the liability for COTS software vulnerabilities.
- B. In-house developed software is inherently less secure.
- C. Exploits for COTS software are well documented and publicly available.
- D. COTS software is inherently less secure.

Answer: C

NEW QUESTION 185

- (Exam Topic 15)

A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

- A. Read
- B. Execute
- C. Write
- D. Append

Answer: C

NEW QUESTION 190

- (Exam Topic 15)

Which of the following is the reason that transposition ciphers are easily recognizable?

- A. Key
- B. Block
- C. Stream
- D. Character

Answer: B

NEW QUESTION 192

- (Exam Topic 15)

A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks, What is the MOST efficient option used to prevent buffer overflow attacks?

- A. Process isolation
- B. Address Space Layout Randomization (ASLR)
- C. Processor states
- D. Access control mechanisms

Answer: B

NEW QUESTION 196

- (Exam Topic 15)

Which of the following is MOST appropriate to collect evidence of a zero-day attack?

- A. Firewall
- B. Honeypot
- C. Antispam
- D. Antivirus

Answer: A

NEW QUESTION 201

- (Exam Topic 15)

What is the benefit of using Network Admission Control (NAC)?

- A. Operating system (OS) versions can be validated prior to allowing network access.
- B. NAC supports validation of the endpoint's security posture prior to allowing the session to go into an authorized state.
- C. NAC can require the use of certificates, passwords, or a combination of both before allowing network admission.
- D. NAC only supports Windows operating systems (OS).

Answer: C

NEW QUESTION 204

- (Exam Topic 15)

Which of the following is the PRIMARY issue when analyzing detailed log information?

- A. Logs may be unavailable when required
- B. Timely review of the data is potentially difficult
- C. Most systems and applications do not support logging
- D. Logs do not provide sufficient details of system and individual activities

Answer: D

NEW QUESTION 207

- (Exam Topic 15)

Which of the following addresses requirements of security assessments during software acquisition?

- A. Software configuration management (SCM)
- B. Data loss prevention (DLP) policy
- C. Continuous monitoring
- D. Software assurance policy

Answer: A

NEW QUESTION 211

- (Exam Topic 15)

A Chief Information Security Officer (CISO) of a firm which decided to migrate to cloud has been tasked with ensuring an optimal level of security. Which of the following would be the FIRST consideration?

- A. Define the cloud migration roadmap and set out which applications and data repositories should be moved into the cloud.
- B. Ensure that the contract between the cloud vendor and the firm clearly defines responsibilities for operating security controls.
- C. Analyze the firm's applications and data repositories to determine the relevant control requirements.
- D. Request a security risk assessment of the cloud vendor be completed by an independent third-party.

Answer: A

NEW QUESTION 212

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 214

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 217

- (Exam Topic 15)

Data remanence is the biggest threat in which of the following scenarios?

- A. A physical disk drive has been overwritten and reused within a datacenter.
- B. A physical disk drive has been degaussed, verified, and released to a third party for destruction.
- C. A flash drive has been overwritten, verified, and reused within a datacenter.
- D. A flash drive has been overwritten and released to a third party for destruction.

Answer: D

NEW QUESTION 219

- (Exam Topic 15)

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

- A. Data Quality Principle

- B. Openness Principle
- C. Purpose Specification Principle
- D. Collection Limitation Principle

Answer: D

NEW QUESTION 223

- (Exam Topic 15)

An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

- A. Default the user to not share any information.
- B. Inform the user of the sharing feature changes after implemented.
- C. Share only what the organization decides is best.
- D. Stop sharing data with the other users.

Answer: D

NEW QUESTION 226

- (Exam Topic 15)

Which of the following is the BEST approach to implement multiple servers on a virtual system?

- A. Implement multiple functions per virtual server and apply the same security configuration for each virtual server.
- B. Implement one primary function per virtual server and apply high security configuration on the host operating system.
- C. Implement one primary function per virtual server and apply individual security configuration for each virtual server.
- D. Implement multiple functions within the same virtual server and apply individual security configurations to each function.

Answer: C

NEW QUESTION 228

- (Exam Topic 15)

Where can the Open Web Application Security Project (OWASP) list of associated vulnerabilities be found?

- A. OWASP Top 10 Project
- B. OWASP Software Assurance Maturity Model (SAMM) Project
- C. OWASP Guide Project
- D. OWASP Mobile Project

Answer: A

NEW QUESTION 233

- (Exam Topic 15)

Which of the following vulnerability assessment activities BEST exemplifies the Examine method of assessment?

- A. Ensuring that system audit logs capture all relevant data fields required by the security controls baseline
- B. Performing Port Scans of selected network hosts to enumerate active services
- C. Asking the Information System Security Officer (ISSO) to describe the organization's patch management processes
- D. Logging into a web server using the default administrator account and a default password

Answer: D

NEW QUESTION 237

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 241

- (Exam Topic 15)

Which of the following types of web-based attack is happening when an attacker is able to send a well-crafted, malicious request to an authenticated user without the user realizing it?

- A. Cross-Site Scripting (XSS)
- B. Cross-Site request forgery (CSRF)
- C. Cross injection
- D. Broken Authentication And Session Management

Answer: B

NEW QUESTION 243

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 248

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 249

- (Exam Topic 15)

An organization recently suffered from a web-application attack that resulted in stolen user session cookie information. The attacker was able to obtain the information when a user's browser executed a script upon visiting a compromised website. What type of attack MOST likely occurred?

- A. Cross-Site Scripting (XSS)
- B. Extensible Markup Language (XML) external entities
- C. SQL injection (SQLI)
- D. Cross-Site Request Forgery (CSRF)

Answer: A

NEW QUESTION 254

- (Exam Topic 15)

The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

- A. Removal of service accounts from review
- B. Segregation of Duties (SoD)
- C. Clear provisioning policies
- D. Frequent audits

Answer: C

NEW QUESTION 258

- (Exam Topic 15)

The Open Web Application Security Project's (OWASP) Software Assurance Maturity Model (SAMM) allows organizations to implement a flexible software security strategy to measure organizational impact based on what risk management aspect?

- A. Risk tolerance
- B. Risk exception
- C. Risk treatment
- D. Risk response

Answer: D

NEW QUESTION 259

- (Exam Topic 15)

A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

- A. Establish a service-oriented architecture (SOA).
- B. Establish a media caching methodology.
- C. Establish relationships with hundreds of Internet service providers (ISP).
- D. Establish a low-latency wide area network (WAN).

Answer: B

NEW QUESTION 262

- (Exam Topic 15)

Which of the following types of datacenter architectures will MOST likely be used in a large SDN and can be extended beyond the datacenter?

- A. iSCSI
- B. FCoE

- C. Three-tiered network
- D. Spine and leafE Top-of-rack switching

Answer: B

NEW QUESTION 267

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 269

- (Exam Topic 15)

A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

- A. Use limitation
- B. Individual participation
- C. Purpose specification
- D. Collection limitation

Answer: D

NEW QUESTION 272

- (Exam Topic 15)

Which of the following is the MOST common use of the Online Certificate Status Protocol (OCSP)?

- A. To obtain the expiration date of an X.509 digital certificate
- B. To obtain the revocation status of an X.509 digital certificate
- C. To obtain the author name of an X.509 digital certificate
- D. To verify the validity of an X.509 digital certificate

Answer: D

NEW QUESTION 277

- (Exam Topic 15)

An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.

Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

- A. Update the Network Address Translation (NAT) table.
- B. Update Domain Name System (DNS) server addresses with domain registrar.
- C. Update the Border Gateway Protocol (BGP) autonomous system number.
- D. Update the web server network adapter configuration.

Answer: B

NEW QUESTION 280

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 281

- (Exam Topic 15)

Configuring a Wireless Access Point (WAP) with the same Service Set Identifier (SSID) as another WAP in order to have users unknowingly connect is referred to as which of the following?

- A. Jamming
- B. Man-in-the-Middle (MITM)
- C. War driving
- D. Internet Protocol (IP) spoofing

Answer: B

NEW QUESTION 282

- (Exam Topic 15)

Which of the following is a key responsibility for a data steward assigned to manage an enterprise data lake?

- A. Ensure proper business definition, value, and usage of data collected and stored within the enterprise data lake.
- B. Ensure proper and identifiable data owners for each data element stored within an enterprise data lake.
- C. Ensure adequate security controls applied to the enterprise data lake.
- D. Ensure that any data passing within remit is being used in accordance with the rules and regulations of the business.

Answer: A

NEW QUESTION 285

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 289

- (Exam Topic 15)

What is the FIRST step in risk management?

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

Answer: C

NEW QUESTION 293

- (Exam Topic 15)

A subscription service which provides power, climate control, raised flooring, and telephone wiring but NOT the computer and peripheral equipment is BEST described as a:

- A. warm site.
- B. reciprocal site.
- C. sicold site.
- D. hot site.

Answer: C

NEW QUESTION 297

- (Exam Topic 15)

Which of the following is a correct feature of a virtual local area network (VLAN)?

- A. A VLAN segregates network traffic therefore information security is enhanced significantly.
- B. Layer 3 routing is required to allow traffic from one VLAN to another.
- C. VLAN has certain security features such as where the devices are physically connected.
- D. There is no broadcast allowed within a single VLAN due to network segregation.

Answer: A

NEW QUESTION 298

- (Exam Topic 15)

What does the result of Cost-Benefit Analysis (C8A) on new security initiatives provide?

- A. Quantifiable justification
- B. Baseline improvement
- C. Risk evaluation
- D. Formalized acceptance

Answer: A

NEW QUESTION 302

- (Exam Topic 15)

The security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network. Which solution is MOST effective at discovering a successful network breach?

- A. Deploying a honeypot
- B. Developing a sandbox
- C. Installing an intrusion prevention system (IPS)
- D. Installing an intrusion detection system (IDS)

Answer: A

NEW QUESTION 303

- (Exam Topic 15)

What is the FIRST step in developing a patch management plan?

- A. Subscribe to a vulnerability subscription service.
- B. Develop a patch testing procedure.
- C. Inventory the hardware and software used.
- D. Identify unnecessary services installed on systems.

Answer: B

NEW QUESTION 304

- (Exam Topic 15)

A Chief Information Officer (CIO) has delegated responsibility of their system security to the head of the information technology (IT) department. While corporate policy dictates that only the CIO can make decisions on the level of data protection required, technical implementation decisions are done by the head of the IT department. Which of the following BEST describes the security role filled by the head of the IT department?

- A. System analyst
- B. System security officer
- C. System processor
- D. System custodian

Answer: D

NEW QUESTION 305

- (Exam Topic 15)

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

Answer: D

NEW QUESTION 307

- (Exam Topic 15)

A software development company found odd behavior in some recently developed software, creating a need for a more thorough code review. What is the MOST effective argument for a more thorough code review?

- A. It will increase flexibility of the applications developed.
- B. It will increase accountability with the customers.
- C. It will impede the development process.
- D. It will reduce the potential for vulnerabilities.

Answer: D

NEW QUESTION 308

- (Exam Topic 15)

When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

- A. Requirements
- B. Risk assessment
- C. Due diligence
- D. Planning

Answer: B

NEW QUESTION 309

- (Exam Topic 15)

The quality assurance (QA) department is short-staffed and is unable to test all modules before the anticipated release date of an application. What security control is MOST likely to be violated?

- A. Separation of environments
- B. Program management
- C. Mobile code controls
- D. Change management

Answer: D

NEW QUESTION 313

- (Exam Topic 15)

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

- A. Identify team members.
- B. Define the scope.

- C. Notify system administrators.
- D. Collect evidence.

Answer: B

NEW QUESTION 315

- (Exam Topic 15)

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

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

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

Answer: B

NEW QUESTION 319

- (Exam Topic 15)

An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

- A. Cross-Site Scripting (XSS)
- B. Pass the ticket
- C. Brute force
- D. Hash collision

Answer: B

NEW QUESTION 323

- (Exam Topic 15)

Of the following, which BEST provides non- repudiation with regards to access to a server room?

- A. Fob and Personal Identification Number (PIN)
- B. Locked and secured cages
- C. Biometric readers
- D. Proximity readers

Answer: C

NEW QUESTION 328

- (Exam Topic 15)

Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

- A. Audit
- B. Compliance
- C. Legal
- D. Security

Answer: C

NEW QUESTION 333

- (Exam Topic 15)

Which of the following BEST ensures the integrity of transactions to intended recipients?

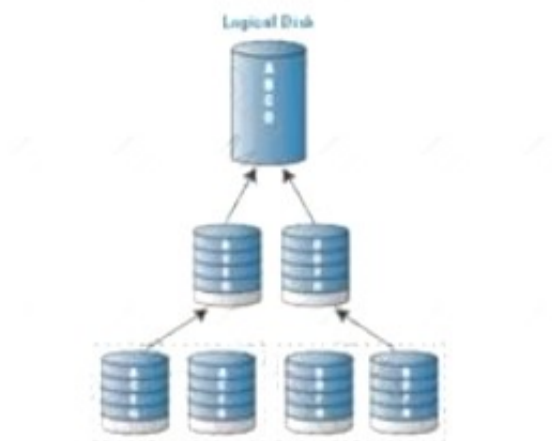
- A. Public key infrastructure (PKI)
- B. Blockchain technology
- C. Pre-shared key (PSK)
- D. Web of trust

Answer: A

NEW QUESTION 337

- (Exam Topic 15)

Which Redundant Array c/ Independent Disks (RAID) Level does the following diagram represent?



- A. RAID 0
- B. RAID 1
- C. RAID 5
- D. RAID 10

Answer: D

NEW QUESTION 339

- (Exam Topic 15)

Which of the following is the BEST option to reduce the network attack surface of a system?

- A. Ensuring that there are no group accounts on the system
- B. Removing unnecessary system user accounts
- C. Disabling unnecessary ports and services
- D. Uninstalling default software on the system

Answer: C

NEW QUESTION 343

- (Exam Topic 15)

An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

- A. 1
- B. 2
- C. 3

Answer: A

NEW QUESTION 346

- (Exam Topic 15)

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

Answer: D

NEW QUESTION 351

- (Exam Topic 15)

A large manufacturing organization arranges to buy an industrial machine system to produce a new line of products. The system includes software provided to the vendor by a thirdparty organization. The financial risk to the manufacturing organization starting production is high. What step should the manufacturing organization take to minimize its financial risk in the new venture prior to the purchase?

- A. Hire a performance tester to execute offline tests on a system.
- B. Calculate the possible loss in revenue to the organization due to software bugs and vulnerabilities, and compare that to the system's overall price.
- C. Place the machine behind a Layer 3 firewall.
- D. Require that the software be thoroughly tested by an accredited independent software testing company.

Answer: B

NEW QUESTION 356

- (Exam Topic 15)

What is the MOST common security risk of a mobile device?

- A. Insecure communications link
- B. Data leakage
- C. Malware infection
- D. Data spoofing

Answer: C

NEW QUESTION 358

- (Exam Topic 15)

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

Answer: A

NEW QUESTION 359

- (Exam Topic 15)

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

This is an example of which type of network topology?

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

Answer: A

NEW QUESTION 364

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 365

- (Exam Topic 15)

What is the second phase of public key infrastructure (PKI) key/certificate life-cycle management?

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

Answer: A

NEW QUESTION 366

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 369

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 372

- (Exam Topic 15)

When developing an organization's information security budget, it is important that the

- A. expected risk can be managed appropriately with the funds allocated.
- B. requested funds are at an equal amount to the expected cost of breaches.
- C. requested funds are part of a shared funding pool with other areas.
- D. expected risk to the organization does not exceed the funds allocated.

Answer: A

NEW QUESTION 374

- (Exam Topic 15)

The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

- A. Skill set and training
- B. Headcount and capacity
- C. Tools and technologies
- D. Scope and service catalog

Answer: C

NEW QUESTION 375

- (Exam Topic 15)

A hacker can use a lockout capability to start which of the following attacks?

- A. Denial of service (DoS)
- B. Dictionary
- C. Ping flood
- D. Man-in-the-middle (MITM)

Answer: A

NEW QUESTION 379

- (Exam Topic 15)

An organization wants a service provider to authenticate users via the users' organization domain credentials. Which markup language should the organization's security personnel use to support the integration?

- A. Security Assertion Markup Language (SAML)
- B. YAML Ain't Markup Language (YAML)
- C. Hypertext Markup Language (HTML)
- D. Extensible Markup Language (XML)

Answer: A

NEW QUESTION 384

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 386

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 389

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 391

- (Exam Topic 15)

A security engineer is assigned to work with the patch and vulnerability management group. The deployment of a new patch has been approved and needs to be applied.

The research is complete, and the security engineer has provided recommendations. Where should the patch be applied FIRST?

- A. Server environment
- B. Desktop environment
- C. Lower environment
- D. Production environment

Answer: C

NEW QUESTION 393

- (Exam Topic 15)

To monitor the security of buried data lines inside the perimeter of a facility, which of the following is the MOST effective control?

- A. Fencing around the facility with closed-circuit television (CCTV) cameras at all entry points
- B. Ground sensors installed and reporting to a security event management (SEM) system
- C. Steel casing around the facility ingress points
- D. regular sweeps of the perimeter, including manual inspection of the cable ingress points

Answer: D

NEW QUESTION 397

- (Exam Topic 15)

A web developer is completing a new web application security checklist before releasing the application to production. the task of disabling unnecessary services is on the checklist. Which web application threat is being mitigated by this action?

- A. Security misconfiguration
- B. Sensitive data exposure
- C. Broken access control
- D. Session hijacking

Answer: B

NEW QUESTION 399

- (Exam Topic 15)

The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery. Which of the following is the MOST challenging aspect of this investigation?

- A. SCADA network latency
- B. Group policy implementation
- C. Volatility of data
- D. Physical access to the system

Answer: C

NEW QUESTION 402

- (Exam Topic 15)

Which of the following BEST describes the use of network architecture in reducing corporate risks associated with mobile devices?

- A. Maintaining a "closed applications model on all mobile devices depends on demilitarized Zone (DM2) servers
- B. Split tunneling enabled for mobile devices improves demilitarized zone (DMZ) security posture
- C. Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices
- D. Applications that manage mobile devices are located in an Internet demilitarized zone (DMZ)

Answer: C

NEW QUESTION 406

- (Exam Topic 15)

Which of the following is a security weakness in the evaluation of common criteria (CC) products?

- A. The manufacturer can state what configuration of the product is to be evaluated.
- B. The product can be evaluated by labs in other countries.
- C. The Target of Evaluation's (TOE) testing environment is identical to the operating environment
- D. The evaluations are expensive and time-consuming to perform.

Answer: A

NEW QUESTION 411

- (Exam Topic 15)

What is the MAIN purpose of a security assessment plan?

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

Answer: B

NEW QUESTION 415

- (Exam Topic 15)

What is the overall goal of software security testing?

- A. Identifying the key security features of the software
- B. Ensuring all software functions perform as specified
- C. Reducing vulnerabilities within a software system
- D. Making software development more agile

Answer: B

NEW QUESTION 420

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 421

- (Exam Topic 15)

A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

- A. Bitlocker
- B. Trusted Platform Module (TPM)
- C. Virtual storage array network (VSAN)
- D. Hardware security module (HSM)

Answer: D

NEW QUESTION 424

- (Exam Topic 15)

Which security feature fully encrypts code and data as it passes to the servers and only decrypts below the hypervisor layer?

- A. File-system level encryption
- B. Transport Layer Security (TLS)
- C. Key management service
- D. Trusted execution environments

Answer: D

NEW QUESTION 429

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 433

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 436

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 441

- (Exam Topic 15)

What is a security concern when considering implementing software-defined networking (SDN)?

- A. It increases the attack footprint.
- B. It uses open source protocols.
- C. It has a decentralized architecture.
- D. It is cloud based.

Answer: C

NEW QUESTION 444

- (Exam Topic 15)

Which of the following determines how traffic should flow based on the status of the infrastructure true?

- A. Application plane
- B. Data plane
- C. Control plane
- D. Traffic plane

Answer: D

NEW QUESTION 448

- (Exam Topic 15)

Which of the following techniques evaluates the secure Bet principles of network or software architectures?

- A. Threat modeling
- B. Risk modeling
- C. Waterfall method
- D. Fuzzing

Answer: A

NEW QUESTION 451

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 456

- (Exam Topic 15)

An organization outgrew its internal data center and is evaluating third-party hosting facilities. In this evaluation, which of the following is a PRIMARY factor for selection?

- A. Facility provides an acceptable level of risk
- B. Facility provides disaster recovery (DR) services
- C. Facility provides the most cost-effective solution
- D. Facility has physical access protection measures

Answer: C

NEW QUESTION 457

- (Exam Topic 15)

A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to on and security However, an attacker was able to spoof a registered account on the network and query the SAML provider.

What is the MOST common attack leverage against this flaw?

- A. Attacker forges requests to authenticate as a different user.
- B. Attacker leverages SAML assertion to register an account on the security domain.
- C. Attacker conducts denial-of-service (DoS) against the security domain by authenticating as the same user repeatedly.

D. Attacker exchanges authentication and authorization data between security domains.

Answer: A

NEW QUESTION 458

- (Exam Topic 15)

Which of the following is the MOST effective corrective control to minimize the effects of a physical intrusion?

- A. Automatic videotaping of a possible intrusion
- B. Rapid response by guards or police to apprehend a possible intruder
- C. Activating bright lighting to frighten away a possible intruder
- D. Sounding a loud alarm to frighten away a possible intruder

Answer: C

NEW QUESTION 462

- (Exam Topic 15)

What is the HIGHEST priority in agile development?

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

Answer: C

NEW QUESTION 467

- (Exam Topic 15)

Which of the following contributes MOST to the effectiveness of a security officer?

- A. Understanding the regulatory environment
- B. Developing precise and practical security plans
- C. Integrating security into the business strategies
- D. Analyzing the strengths and weakness of the organization

Answer: A

NEW QUESTION 472

- (Exam Topic 15)

Which of the following is an important design feature for the outer door of a mantrap?

- A. Allow it to be opened by an alarmed emergency button.
- B. Do not allow anyone to enter it alone.
- C. Do not allow it to be observed by closed-circuit television (CCTV) cameras.
- D. Allow it be opened when the inner door of the mantrap is also open

Answer: D

NEW QUESTION 475

- (Exam Topic 15)

A company-wide penetration test result shows customers could access and read files through a web browser. Which of the following can be used to mitigate this vulnerability?

- A. Enforce the chmod of files to 755.
- B. Enforce the control of file directory listings.
- C. Implement access control on the web server.
- D. Implement Secure Sockets Layer (SSL) certificates throughout the web server.

Answer: B

NEW QUESTION 477

- (Exam Topic 15)

Which of the following is a covert channel type?

- A. Storage
- B. Pipe
- C. Memory
- D. Monitoring

Answer: A

NEW QUESTION 482

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 486

- (Exam Topic 15)

Which of the following should be included in a good defense-in-depth strategy provided by object-oriented programming for software deployment?

- A. Polyinstantiation
- B. Polymorphism
- C. Encapsulation
- D. Inheritance

Answer: A

NEW QUESTION 491

- (Exam Topic 15)

When are security requirements the LEAST expensive to implement?

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

Answer: D

NEW QUESTION 492

- (Exam Topic 15)

Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

- A. Trusted Computing Base (TCB)
- B. Time separation
- C. Security kernel
- D. Reference monitor

Answer: C

NEW QUESTION 497

- (Exam Topic 15)

Which of the following is a canon of the (ISC)2 Code of Ethics?

- A. Integrity first, association before self, and excellence in all we do
- B. Perform all professional activities and duties in accordance with all applicable laws and the highest ethical standards.
- C. Provide diligent and competent service to principals.
- D. Cooperate with others in the interchange of knowledge and ideas for mutual security.

Answer: C

NEW QUESTION 499

- (Exam Topic 15)

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

Answer: D

NEW QUESTION 502

- (Exam Topic 15)

What is the PRIMARY purpose of auditing, as it relates to the security review cycle?

- A. To ensure the organization's controls and policies are working as intended
- B. To ensure the organization can still be publicly traded
- C. To ensure the organization's executive team won't be sued
- D. To ensure the organization meets contractual requirements

Answer: A

NEW QUESTION 507

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 512

- (Exam Topic 15)

What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

- A. Implement egress filtering at the organization's network boundary.
- B. Implement network access control lists (ACL).
- C. Implement a web application firewall (WAF).
- D. Implement an intrusion prevention system (IPS).

Answer: B

NEW QUESTION 513

- (Exam Topic 15)

What is the BEST reason to include supply chain risks in a corporate risk register?

- A. Risk registers help fund corporate supply chain risk management (SCRM) systems.
- B. Risk registers classify and categorize risk and allow risks to be compared to corporate risk appetite.
- C. Risk registers can be used to illustrate residual risk across the company.
- D. Risk registers allow for the transfer of risk to third parties.

Answer: B

NEW QUESTION 517

- (Exam Topic 15)

At which phase of the software assurance life cycle should risks associated with software acquisition strategies be identified?

- A. Follow-on phase
- B. Planning phase
- C. Monitoring and acceptance phase
- D. Contracting phase

Answer: C

NEW QUESTION 518

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 519

- (Exam Topic 15)

In an IDEAL encryption system, who has sole access to the decryption key?

- A. System owner
- B. Data owner
- C. Data custodian
- D. System administrator

Answer: B

NEW QUESTION 523

- (Exam Topic 15)

A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several 'open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

- A. Mandate that all open-source components be approved by the Information Security Manager (ISM).
- B. Scan all open-source components for security vulnerabilities.
- C. Establish an open-source compliance policy.
- D. Require commercial support for all open-source components.

Answer: C

NEW QUESTION 528

- (Exam Topic 15)

Which of the following statements is MOST accurate regarding information assets?

- A. International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.
- B. S3 Information assets include any information that is valuable to the organization,
- C. Building an information assets register is a resource-intensive job.
- D. Information assets inventory is not required for risk assessment.

Answer: B

NEW QUESTION 532

- (Exam Topic 15)

Which of the following is a secure design principle for a new product?

- A. Build in appropriate levels of fault tolerance.
- B. Utilize obfuscation whenever possible.
- C. Do not rely on previously used code.
- D. Restrict the use of modularization.

Answer: A

NEW QUESTION 537

- (Exam Topic 15)

What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

- A. Risk assessment
- B. Performance testing
- C. Security audit
- D. Risk management

Answer: D

NEW QUESTION 540

- (Exam Topic 15)

What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

- A. Monitoring and identifying system failures, documenting incidents for future analysis, and scheduling patches for systems
- B. Scheduling patches for systems, notifying the help desk, and alerting key personnel
- C. Monitoring and identifying system failures, alerting key personnel, and containing events
- D. Documenting incidents for future analysis, notifying end users, and containing events

Answer: D

NEW QUESTION 543

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 546

- (Exam Topic 15)

Which of the following BEST describes botnets?

- A. Computer systems on the Internet that are set up to trap people who attempt to penetrate other computer system
- B. Set of related programs that protects the resources of a private network from other networks
- C. Small network inserted in a neutral zone between an organization's private network and the outside public network
- D. Groups of computers that are used to launch destructive attacks

Answer: D

NEW QUESTION 547

- (Exam Topic 14)

What is the MOST effective way to determine a mission critical asset in an organization?

- A. Vulnerability analysis
- B. business process analysis
- C. Threat analysis

D. Business risk analysis

Answer: B

NEW QUESTION 548

- (Exam Topic 14)

Which of the following media is LEAST problematic with data remanence?

- A. Dynamic Random Access Memory (DRAM)
- B. Electrically Erasable Programming Read-Only Memory (BPRCM)
- C. Flash memory
- D. Magnetic disk

Answer: A

NEW QUESTION 549

- (Exam Topic 14)

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

Answer: A

NEW QUESTION 550

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 551

- (Exam Topic 14)

copyright provides protection for which of the following?

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

Answer: C

NEW QUESTION 555

- (Exam Topic 14)

Internet protocol security (IPSec), point-to-point tunneling protocol (PPTP), and secure sockets Layer (SSL) all use Which of the following to prevent replay attacks?

- A. Large Key encryption
- B. Single integrity protection
- C. Embedded sequence numbers
- D. Randomly generated nonces

Answer: C

NEW QUESTION 556

- (Exam Topic 14)

For the purpose of classification, which of the following is used to divide trust domain and trust boundaries?

- A. Network architecture
- B. Integrity
- C. Identity Management (IdM)
- D. Confidentiality management

Answer: A

NEW QUESTION 561

- (Exam Topic 14)

Which of the following techniques is effective to detect taps in fiber optic cables?

- A. Taking baseline signal level of the cable
- B. Measuring signal through external oscillator solution devices
- C. Outlining electromagnetic field strength
- D. Performing network vulnerability scanning

Answer: B

NEW QUESTION 562

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 567

- (Exam Topic 14)

How long should the records on a project be retained?

- A. For the duration of the project, or at the discretion of the record owner
- B. Until they are no longer useful or required by policy
- C. Until five years after the project ends, then move to archives
- D. For the duration of the organization fiscal year

Answer: B

NEW QUESTION 569

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 570

- (Exam Topic 14)

Which of the following encryption types is used in Hash Message Authentication Code (HMAC) for key distribution?

- A. Symmetric
- B. Asymmetric
- C. Ephemeral
- D. Permanent

Answer: A

Explanation:

Reference: <https://www.brainscape.com/flashcards/cryptography-message-integrity-6886698/packs/10957693>

NEW QUESTION 572

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 575

- (Exam Topic 14)

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

Answer: D

NEW QUESTION 577

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 581

- (Exam Topic 14)

Which of the following types of data would be MOST difficult to detect by a forensic examiner?

- A. Slack space data
- B. Steganographic data
- C. File system deleted data
- D. Data stored with a different file type extension

Answer: C

NEW QUESTION 586

- (Exam Topic 14)

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

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

Answer: B

Explanation:

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

NEW QUESTION 587

- (Exam Topic 14)

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.

Answer: C

NEW QUESTION 589

- (Exam Topic 14)

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)

Answer: A

NEW QUESTION 593

- (Exam Topic 14)

Which of the following practices provides the development team with a definition of security and identification of threats in designing software?

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

Answer: C

NEW QUESTION 597

- (Exam Topic 14)

What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

- A. Manual inspections and reviews
- B. Penetration testing

- C. Threat modeling
- D. Source code review

Answer: C

NEW QUESTION 599

- (Exam Topic 14)

Which of the following is the PRIMARY consideration when determining the frequency an automated control should be assessed or monitored?

- A. The complexity of the automated control
- B. The level of automation of the control
- C. The range of values of the automated control
- D. The volatility of the automated control

Answer: B

NEW QUESTION 600

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 604

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 609

- (Exam Topic 14)

An organization operates a legacy Industrial Control System (ICS) to support its core business service, which cannot be replaced. Its management MUST be performed remotely through an administrative console software, which in turn depends on an old version of the Java Runtime Environment (JRE) 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 migrate to a modern technology
- D. Deploy a restrictive proxy between all clients and the vulnerable management station

Answer: B

NEW QUESTION 614

- (Exam Topic 14)

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.

Answer: C

NEW QUESTION 616

- (Exam Topic 14)

What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

- A. Exercise due diligence when deciding to circumvent host government requests.
- B. Become familiar with the means in which the code of ethics is applied and considered.
- C. Complete the assignment based on the customer's wishes.
- D. Execute according to the professional's comfort level with the code of ethics.

Answer: B

NEW QUESTION 620

- (Exam Topic 14)

Which layer of the Open system Interconnect (OSI) model is responsible for secure data transfer between applications, flow control, and error detection and correction?

- A. Layer 2
- B. Layer 4
- C. Layer 5
- D. Layer 6

Answer: B

NEW QUESTION 623

- (Exam Topic 14)

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 on employee activities

Answer: A

NEW QUESTION 625

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 630

- (Exam Topic 14)

Which of the following is the BEST defense against password guessing?

- A. Limit external connections to the network.
- B. Disable the account after a limited number of unsuccessful attempts.
- C. Force the password to be changed after an invalid password has been entered.
- D. Require a combination of letters, numbers, and special characters in the password.

Answer: D

NEW QUESTION 635

- (Exam Topic 14)

Which of the following open source software issues pose the MOST risk to an application?

- A. The software is beyond end of life and the vendor is out of business.
- B. The software is not used or popular in the development community.
- C. The software has multiple Common Vulnerabilities and Exposures (CVE) and only some are remediated.
- D. The software has multiple Common Vulnerabilities and Exposures (CVE) but the CVEs are classified as low risks.

Answer: D

NEW QUESTION 636

- (Exam Topic 14)

Which of the following is the BEST statement for a professional to include as part of business continuity (BC) procedure?

- A. A full data backup must be done upon management request.
- B. An incremental data backup must be done upon management request.
- C. A full data backup must be done based on the needs of the business.
- D. An incremental data backup must be done after each system change.

Answer: D

NEW QUESTION 639

- (Exam Topic 14)

An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.

Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

- A. The audit assessment has been conducted by an independent assessor.
- B. The audit reports have been signed by the third-party senior management.
- C. The audit reports have been issued in the last six months.
- D. The audit assessment has been conducted by an international audit firm.

Answer: A

NEW QUESTION 642

- (Exam Topic 14)

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

- A. Ensure 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.

Answer: C

NEW QUESTION 646

- (Exam Topic 14)

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)

Answer: C

NEW QUESTION 648

- (Exam Topic 14)

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

- A. Intrusion Prevention System (IPS)
- B. Denial of Service (DoS) protection solution
- C. One-time Password (OTP) token
- D. Web Application Firewall (WAF)

Answer: A

NEW QUESTION 652

- (Exam Topic 14)

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 endpoints
- D. Enforce port security on access switches

Answer: A

NEW QUESTION 656

- (Exam Topic 14)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 661

- (Exam Topic 14)

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

Answer: B

NEW QUESTION 665

- (Exam Topic 14)

Which of the following is a PRIMARY challenge when running a penetration test?

- A. Determining the cost
- B. Establishing a business case
- C. Remediating found vulnerabilities
- D. Determining the depth of coverage

Answer: D

NEW QUESTION 667

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 668

- (Exam Topic 14)

As users switch roles within an organization, their accounts are given additional permissions to perform the duties of their new position. After a recent audit, it was discovered that many of these accounts maintained their old permissions as well. The obsolete permissions identified by the audit have been remediated and accounts have only the appropriate permissions to complete their jobs.

Which of the following is the BEST way to prevent access privilege creep?

- A. Implementing Identity and Access Management (IAM) solution
- B. Time-based review and certification
- C. Internet audit
- D. Trigger-based review and certification

Answer: A

NEW QUESTION 669

- (Exam Topic 14)

When deploying an 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

Answer: A

NEW QUESTION 670

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 673

- (Exam Topic 14)

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

Answer: B

NEW QUESTION 675

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 676

- (Exam Topic 14)

A security engineer is designing a Customer Relationship Management (CRM) application for a third-party vendor. In which phase of the System Development Life Cycle (SDLC) will it be MOST beneficial to conduct a data sensitivity assessment?

- A. Development / Acquisition
- B. Initiation
- C. Enumeration
- D. Operation / Maintenance

Answer: B

NEW QUESTION 678

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 679

- (Exam Topic 14)

Which of the following is a peer entity authentication method for Point-to-Point Protocol (PPP)?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Message Authentication Code (MAC)
- C. Transport Layer Security (TLS) handshake protocol
- D. Challenge-response authentication mechanism

Answer: A

NEW QUESTION 684

- (Exam Topic 14)

An analysis finds unusual activity coming from a computer that was thrown away several months prior, which of the following steps ensure the proper removal of the system?

- A. Deactivation
- B. Decommission
- C. Deploy
- D. Procure

Answer: B

NEW QUESTION 689

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 693

- (Exam Topic 14)

When designing an Occupant Emergency plan (OEP) for United States (US) Federal government facilities, what factor must be considered?

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

Answer: A

NEW QUESTION 696

- (Exam Topic 14)

Following a penetration test, what should an organization do FIRST?

- A. Review all security policies and procedures.

- B. Ensure staff is trained in security.
- C. Determine if you need to conduct a full security assessment.
- D. Evaluate the problems identified in the test result.

Answer: D

NEW QUESTION 697

- (Exam Topic 14)
Which type of test suite should be run for fast feedback during application development?

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

Answer: C

NEW QUESTION 698

- (Exam Topic 14)
Match the level of evaluation to the correct common criteria (CC) assurance level.
Drag each level of evaluation on the left to is corresponding CC assurance level on the right

Level of Evaluation

Structurally tested

Methodically tested and checked

Methodically designed, tested, and reviewed

Functionally tested

Semiformally verified design and tested

Formally verified design and tested

Semiformally designed and tested

Assurance Level

1

2

3

4

5

6

7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Level of Evaluation

Structurally tested

Methodically tested and checked

Methodically designed, tested, and reviewed

Functionally tested

Semiformally verified design and tested

Formally verified design and tested

Semiformally designed and tested

Assurance Level

1

2

3

4

5

6

7

Functionally tested

Structurally tested

Methodically tested and checked

Methodically designed, tested, and reviewed

Semiformally designed and tested

Semiformally verified design and tested

Formally verified design and tested

NEW QUESTION 702

- (Exam Topic 14)
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

Answer: B

NEW QUESTION 706

- (Exam Topic 14)

Which of the following is the MOST important action regarding authentication?

- A. Granting access rights
- B. Enrolling in the system
- C. Establishing audit controls
- D. Obtaining executive authorization

Answer: B

NEW QUESTION 710

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 714

- (Exam Topic 14)

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.

Answer: D

NEW QUESTION 716

- (Exam Topic 14)

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)

Answer: B

NEW QUESTION 719

- (Exam Topic 14)

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

Answer: B

NEW QUESTION 724

- (Exam Topic 14)

Which of the following is true of Service Organization Control (SOC) reports?

- A. SOC 1 Type 2 reports assess the security, confidentiality, integrity, and availability of an organization's controls
- B. SOC 2 Type 2 reports include information of interest to the service organization's management
- C. SOC 2 Type 2 reports assess internal controls for financial reporting
- D. SOC 3 Type 2 reports assess internal controls for financial reporting

Answer: B

Explanation:

Reference:

http://ssae16.businesscatalyst.com/SSAE16_reports.html

NEW QUESTION 729

- (Exam Topic 14)

Which of the following is applicable to a publicly held company concerned about information handling and storage requirement specific to the financial reporting?

- A. Privacy Act of 1974
- B. Clinger-Cohan Act of 1996
- C. Sarbanes-Oxley (SOX) Act of 2002
- D. International Organization for Standardization (ISO) 27001

Answer: C

NEW QUESTION 732

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 737

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 738

- (Exam Topic 14)

Which of the following will help prevent improper session handling?

- A. Ensure that all UIWebView calls do not execute without proper input validation.
- B. Ensure that tokens are sufficiently long, complex, and pseudo-random.
- C. Ensure JavaScript and plugin support is disabled.
- D. Ensure that certificates are valid and fail closed.

Answer: B

NEW QUESTION 740

- (Exam Topic 14)

The threat modeling identifies a man-in-the-middle (MITM) exposure. Which countermeasure should the information system security officer (ISSO) select to mitigate the risk of a protected Health information (PHI) data leak?

- A. Auditing
- B. Anonymization
- C. Privacy monitoring
- D. Data retention

Answer: B

NEW QUESTION 745

- (Exam Topic 14)

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

- A. To standardize on a single vendor
- B. To ensure isolation of management traffic
- C. To maximize data plane efficiency
- D. To reduce the risk of configuration errors

Answer: C

NEW QUESTION 749

- (Exam Topic 14)

Which of the following activities is MOST likely to be performed during a vulnerability assessment?

- A. Establish caller authentication procedures to verify the identities of users.
- B. Analyze the environment by conducting interview sessions with relevant parties.
- C. Document policy exceptions required to access systems in non-compliant areas.
- D. Review professorial credentials of the vulnerability assessment team or vendor.

Answer: D

NEW QUESTION 752

- (Exam Topic 14)

What is the threat modeling order using process for Attack simulation and threat analysis (PASTA)?

- A. Application decomposition, threat analysis, vulnerability detection, attack enumeration, risk/impact analysis
- B. Threat analysis, vulnerability detection, application decomposition, attack enumeration, risk/Impact analysis
- C. Risk/impact analysis, application decomposition, threat analysis, vulnerability detection, attack enumeration
- D. Application decomposition, threat analysis, risk/impact analysis, vulnerability detection, attack enumeration

Answer: A

NEW QUESTION 757

- (Exam Topic 14)

Which of the following is the key requirement for test results when implementing forensic procedures?

- A. The test results must be cost-effective.
- B. The test result must be authorized.
- C. The test results must be quantifiable.
- D. The test results must be reproducible.

Answer: B

NEW QUESTION 758

- (Exam Topic 14)

Which of the following is an advantage of Secure Shell (SSH)?

- A. It operates at the network layer.
- B. It encrypts transmitted User ID and passwords.
- C. It uses challenge-response to authenticate each party.
- D. It uses the International Data Encryption Algorithm (IDEA) for data privacy.

Answer: C

NEW QUESTION 759

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 764

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 768

- (Exam Topic 14)

Which of the following techniques BEST prevents buffer overflows?

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

Answer: B

Explanation:

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

NEW QUESTION 772

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 775

- (Exam Topic 14)

Which of the following statements is TRUE regarding equivalence class testing?

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

Answer: C

NEW QUESTION 778

- (Exam Topic 14)

Which inherent password weakness does a One Time Password (OTP) generator overcome?

- A. Static passwords must be changed frequently.
- B. Static passwords are too predictable.
- C. Static passwords are difficult to generate.
- D. Static passwords are easily disclosed.

Answer: D

NEW QUESTION 779

- (Exam Topic 14)

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 error MOST likely occur?

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

Answer: A

NEW QUESTION 784

- (Exam Topic 14)

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.

Answer: B

NEW QUESTION 789

- (Exam Topic 14)

A security professional should consider the protection of which of the following elements FIRST when developing a defense-in-depth strategy for a mobile workforce?

- A. Network perimeters
- B. Demilitarized Zones (DM2)
- C. Databases and back-end servers
- D. End-user devices

Answer: D

NEW QUESTION 794

- (Exam Topic 14)

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

Answer: B

NEW QUESTION 795

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 796

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 798

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 800

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 803

- (Exam Topic 13)

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

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

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 805

- (Exam Topic 13)

What is the foundation of cryptographic functions?

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

Answer: D

NEW QUESTION 809

- (Exam Topic 13)

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.

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 811

- (Exam Topic 13)

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

Answer: D

NEW QUESTION 816

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 820

- (Exam Topic 13)

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)

Answer: B

NEW QUESTION 824

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 829

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 833

- (Exam Topic 13)

Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?

- A. Standardized configurations for devices
- B. Standardized patch testing equipment
- C. Automated system patching

D. Management support for patching

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 838

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 843

- (Exam Topic 13)

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

Answer: B

NEW QUESTION 845

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 849

- (Exam Topic 13)

A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

- A. Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)
- B. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- C. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
- D. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 851

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 855

- (Exam Topic 13)

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

Answer: A

NEW QUESTION 857

- (Exam Topic 13)

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

Answer: A

NEW QUESTION 862

- (Exam Topic 13)

Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP). Which of the following represents a valid measure to help protect the network against unauthorized access?

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

Answer: B

NEW QUESTION 865

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 870

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 871

- (Exam Topic 13)

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

Answer: B

NEW QUESTION 873

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 876

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 879

- (Exam Topic 13)

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

Answer: A

NEW QUESTION 881

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

- * CISSP Questions and Answers Updated Frequently
- * CISSP Practice Questions Verified by Expert Senior Certified Staff
- * CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP Practice Test Here](#)