



ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1

- (Exam Topic 15)

What is the FIRST step when developing an Information Security Continuous Monitoring (ISCM) program?

- A. Establish an ISCM technical architecture.
- B. Collect the security-related information required for metrics, assessments, and reporting.
- C. Establish an ISCM program determining metrics, status monitoring frequencies, and control assessment frequencies.
- D. Define an ISCM strategy based on risk tolerance.

Answer: D

NEW QUESTION 2

- (Exam Topic 15)

In addition to life, protection of which of the following elements is MOST important when planning a data center site?

- A. Data and hardware
- B. Property and operations
- C. Profits and assets
- D. Resources and reputation

Answer: D

NEW QUESTION 3

- (Exam Topic 15)

Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

- A. Client-to-site VPN
- B. Third-party VPN service
- C. Site-to-site VPN
- D. Split-tunnel VPN

Answer: C

NEW QUESTION 4

- (Exam Topic 15)

Which of the following is an important requirement when designing a secure remote access system?

- A. Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated.
- B. Provide privileged access rights to computer files and systems.
- C. Ensure that logging and audit controls are included.
- D. Reduce administrative overhead through password self service.

Answer: C

NEW QUESTION 5

- (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 6

- (Exam Topic 15)

Which of the following is the top barrier for companies to adopt cloud technology?

- A. Migration period
- B. Data integrity
- C. Cost
- D. Security

Answer: D

NEW QUESTION 7

- (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 8

- (Exam Topic 15)

Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

- A. Group Policy Object (GPO)
- B. Network Access Control (NAC)
- C. Mobile Device Management (MDM)
- D. Privileged Access Management (PAM)

Answer: B

NEW QUESTION 9

- (Exam Topic 15)

Which of the following virtual network configuration options is BEST to protect virtual machines (VM)?

- A. Traffic filtering
- B. Data encryption
- C. Data segmentation
- D. Traffic throttling

Answer: D

NEW QUESTION 10

- (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 10

- (Exam Topic 15)

Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

- A. Check the technical design.
- B. Conduct a site survey.
- C. Categorize assets.
- D. Choose a suitable location.

Answer: A

NEW QUESTION 13

- (Exam Topic 15)

An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP). The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract.

Which of the following MUST be included in the contract?

- A. A detailed overview of all equipment involved in the outsourcing contract
- B. The MSSP having an executive manager responsible for information security
- C. The right to perform security compliance tests on the MSSP's equipment
- D. The right to audit the MSSP's security process

Answer: C

NEW QUESTION 14

- (Exam Topic 15)

A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

- A. Risk avoidance
- B. Security engineering
- C. security awareness
- D. Phishing

Answer: C

NEW QUESTION 15

- (Exam Topic 15)

In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed?

- A. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
- B. Maintain and improve the Business Continuity Management (BCM) system by taking corrective action, based on the results of management review.
- C. Ensure the business continuity policy, controls, processes, and procedures have been implemented.
- D. Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established.

Answer: D

NEW QUESTION 17

- (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)

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

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

Answer: B

NEW QUESTION 24

- (Exam Topic 15)

A customer continues to experience attacks on their email, web, and File Transfer Protocol (FTP) servers. These attacks are impacting their business operations. Which of the following is the BEST recommendation to make?

- A. Configure an intrusion detection system (IDS).
- B. Create a demilitarized zone (DMZ).
- C. Deploy a bastion host.
- D. Setup a network firewall.

Answer: C

NEW QUESTION 27

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 30

- (Exam Topic 15)

Which of the following is the MOST effective preventative method to identify security flaws in software?

- A. Monitor performance in production environments.
- B. Perform a structured code review.
- C. Perform application penetration testing.
- D. Use automated security vulnerability testing tools.

Answer: B

NEW QUESTION 31

- (Exam Topic 15)

What would be the BEST action to take in a situation where collected evidence was left unattended overnight in an unlocked vehicle?

- A. Report the matter to the local police authorities.
- B. Move evidence to a climate-controlled environment.
- C. Re-inventory the evidence and provide it to the evidence custodian.

D. Immediately report the matter to the case supervisor.

Answer: D

NEW QUESTION 32

- (Exam Topic 15)

Which of the following is the MOST effective method of detecting vulnerabilities in web-based applications early in the secure Software Development Life Cycle (SDLC)?

- A. Web application vulnerability scanning
- B. Application fuzzing
- C. Code review
- D. Penetration testing

Answer: C

NEW QUESTION 33

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 38

- (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 41

- (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 45

- (Exam Topic 15)

Why is authentication by ownership stronger than authentication by knowledge?

- A. It is easier to change.
- B. It can be kept on the user's person.
- C. It is more difficult to duplicate.
- D. It is simpler to control.

Answer: B

NEW QUESTION 50

- (Exam Topic 15)

Which of the following implementations will achieve high availability in a website?

- A. Multiple Domain Name System (DNS) entries resolving to the same web server and large amounts of bandwidth
- B. Disk mirroring of the web server with redundant disk drives in a hardened data center
- C. Disk striping of the web server hard drives and large amounts of bandwidth
- D. Multiple geographically dispersed web servers that are configured for failover

Answer: D

NEW QUESTION 52

- (Exam Topic 15)

Which of the following examples is BEST to minimize the attack surface for a customer's private information?

- A. Obfuscation
- B. Collection limitation
- C. Authentication
- D. Data masking

Answer: A

NEW QUESTION 53

- (Exam Topic 15)

Who should formulate conclusions from a particular digital fore Ball, Submit a Toper Of Tags, and the results?

- A. The information security professional's supervisor
- B. Legal counsel for the information security professional's employer
- C. The information security professional who conducted the analysis
- D. A peer reviewer of the information security professional

Answer: B

NEW QUESTION 57

- (Exam Topic 15)

What is the BEST control to be implemented at a login page in a web application to mitigate the ability to enumerate users?

- A. Implement a generic response for a failed login attempt.
- B. Implement a strong password during account registration.
- C. Implement numbers and special characters in the user name.
- D. Implement two-factor authentication (2FA) to login process.

Answer: A

NEW QUESTION 60

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 61

- (Exam Topic 15)

As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem?

- A. Cloud broker
- B. Cloud provider
- C. Cloud consumer
- D. Cloud auditor

Answer: C

NEW QUESTION 64

- (Exam Topic 15)

Which of the following is security control volatility?

- A. A reference to the stability of the security control.
- B. A reference to how unpredictable the security control is.
- C. A reference to the impact of the security control.
- D. A reference to the likelihood of change in the security control.

Answer: D

NEW QUESTION 68

- (Exam Topic 15)

Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

- A. Organizations can only reach a maturity level 3 when using CMMs
- B. CMMs do not explicitly address safety and security
- C. CMMs can only be used for software developed in-house
- D. CMMs are vendor specific and may be biased

Answer: B

NEW QUESTION 71

- (Exam Topic 15)

In supervisory control and data acquisition (SCADA) systems, which of the following controls can be used to reduce device exposure to malware?

- A. Disable all command line interfaces.
- B. Disallow untested code in the execution space of the SCADA device.
- C. Prohibit the use of unsecure scripting languages.
- D. Disable Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port 138 and 139 on the SCADA device.

Answer: B

NEW QUESTION 74

- (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 79

- (Exam Topic 15)

Spyware is BEST described as

- A. data mining for advertising.
- B. a form of cyber-terrorism,
- C. an information gathering technique,
- D. a web-based attack.

Answer: B

NEW QUESTION 80

- (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 81

- (Exam Topic 15)

Which of the following is the MOST important rule for digital investigations?

- A. Ensure event logs are rotated.
- B. Ensure original data is never modified.
- C. Ensure individual privacy is protected.
- D. Ensure systems are powered on.

Answer: C

NEW QUESTION 83

- (Exam Topic 15)

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

- A. Omni
- B. Directional
- C. Yagi
- D. Parabolic

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 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 90

- (Exam Topic 15)

In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below. Which of the following would be a reasonable annual loss expectation?

Availability	60,000
Integrity	10,000
Confidentiality	0
Total Impact	70,000

- A. 140,000
- B. 3,500
- C. 350,000
- D. 14,000

Answer: B

NEW QUESTION 92

- (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 94

- (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 97

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 100

- (Exam Topic 15)

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

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

D. Encryption

Answer: A

NEW QUESTION 102

- (Exam Topic 15)

What is the BEST way to restrict access to a file system on computing systems?

- A. Allow a user group to restrict access.
- B. Use a third-party tool to restrict access.
- C. Use least privilege at each level to restrict access.
- D. Restrict access to all users.

Answer: C

NEW QUESTION 104

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 105

- (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 107

- (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 109

- (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 114

- (Exam Topic 15)

A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

- A. The software has the correct functionality.
- B. The software has been code reviewed.
- C. The software had been branded according to corporate standards.
- D. The software has been signed off for release by the product owner.

Answer: A

NEW QUESTION 117

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 121

- (Exam Topic 15)

- A. Obtain information security management approval.
- B. Maintain the integrity of the application.
- C. Obtain feedback before implementation.
- D. Identify vulnerabilities.

Answer: D

NEW QUESTION 122

- (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 125

- (Exam Topic 15)

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Scope options
- B. Reservation
- C. Dynamic assignment
- D. Exclusion
- E. Static assignment

Answer: B

NEW QUESTION 128

- (Exam Topic 15)

Which of the following is the BEST way to determine the success of a patch management process?

- A. Analysis and impact assessment
- B. Auditing and assessment
- C. Configuration management (CM)
- D. Change management

Answer: A

NEW QUESTION 131

- (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 133

- (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 134

- (Exam Topic 15)

Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

- A. Parallel
- B. Simulation
- C. Table-top
- D. Cut-over

Answer: C

NEW QUESTION 136

- (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 137

- (Exam Topic 15)

When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network. Which of the following will BEST help secure the VoIP network?

- A. Transport Layer Security (TLS)
- B. 802.1x
- C. 802.119
- D. Web application firewall (WAF)

Answer: A

NEW QUESTION 141

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 146

- (Exam Topic 15)

An information security administrator wishes to block peer-to-peer (P2P) traffic over Hypertext Transfer Protocol (HTTP) tunnels. Which of the following layers of the Open Systems Interconnection (OSI) model requires inspection?

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

Answer: A

NEW QUESTION 149

- (Exam Topic 15)

Which of the following is the MOST significant key management problem due to the number of keys created?

- A. Keys are more difficult to provision and
- B. Storage of the keys require increased security
- C. Exponential growth when using asymmetric keys
- D. Exponential growth when using symmetric keys

Answer: B

NEW QUESTION 152

- (Exam Topic 15)

A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

- A. Arraignment
- B. Trial
- C. Sentencing
- D. Discovery

Answer: D

NEW QUESTION 154

- (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 155

- (Exam Topic 15)

In setting expectations when reviewing the results of a security test, which of the following statements is MOST important to convey to reviewers?

- A. The target's security posture cannot be further compromised.
- B. The results of the tests represent a point-in-time assessment of the target(s).
- C. The accuracy of testing results can be greatly improved if the target(s) are properly hardened.
- D. The deficiencies identified can be corrected immediately

Answer: C

NEW QUESTION 156

- (Exam Topic 15)

A hospital has allowed virtual private networking (VPN) access to remote database developers. Upon auditing the internal firewall configuration, the network administrator discovered that split-tunneling was enabled. What is the concern with this configuration?

- A. Remote sessions will not require multi-layer authentication.
- B. Remote clients are permitted to exchange traffic with the public and private network.
- C. Multiple Internet Protocol Security (IPSec) tunnels may be exploitable in specific circumstances.
- D. The network intrusion detection system (NIDS) will fail to inspect Secure Sockets Layer (SSL) traffic.

Answer: C

NEW QUESTION 159

- (Exam Topic 15)

Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

- A. A pre-action system is installed.
- B. An open system is installed.
- C. A dry system is installed.
- D. A wet system is installed.

Answer: C

NEW QUESTION 162

- (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 165

- (Exam Topic 15)

In a large company, a system administrator needs to assign users access to files using Role Based Access Control (RBAC). Which option is an example of RBAC?

- A. Mowing users access to files based on their group membership
- B. Allowing users access to files based on username
- C. Allowing users access to files based on the users location at time of access
- D. Allowing users access to files based on the file type

Answer: A

NEW QUESTION 166

- (Exam Topic 15)

Which of the following will an organization's network vulnerability testing process BEST enhance?

- A. Firewall log review processes

- B. Asset management procedures
- C. Server hardening processes
- D. Code review procedures

Answer: C

NEW QUESTION 169

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 173

- (Exam Topic 15)

Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this TAM action?

- A. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to services.
- B. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to services.
- C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identityprovider (IdP) and allows access to resources.
- D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to resources.

Answer: A

NEW QUESTION 176

- (Exam Topic 15)

Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

- A. File Integrity Checker
- B. Security information and event management (SIEM) system
- C. Audit Logs
- D. Intrusion detection system (IDS)

Answer: A

NEW QUESTION 180

- (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 182

- (Exam Topic 15)

A Distributed Denial of Service (DDoS) attack was carried out using malware called Mirai to create a large-scale command and control system to launch a botnet. Which of the following devices were the PRIMARY sources used to generate the attack traffic?

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

Answer: A

NEW QUESTION 185

- (Exam Topic 15)

An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

- A. Health Insurance Portability and Accountability Act (HIPAA)
- B. Service Organization Control (SOC) 2
- C. Payment Card Industry (PCI)
- D. Information Assurance Technical Framework (IATF)

Answer: B

NEW QUESTION 188

- (Exam Topic 15)

Which of the following is required to verify the authenticity of a digitally signed document?

- A. Digital hash of the signed document
- B. Sender's private key
- C. Recipient's public key
- D. Agreed upon shared secret

Answer: A

NEW QUESTION 190

- (Exam Topic 15)

Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

- A. Disaster
- B. Catastrophe
- C. Crisis
- D. Accident

Answer: B

NEW QUESTION 191

- (Exam Topic 15)

The ability to send malicious code, generally in the form of a client side script, to a different end user is categorized as which type of vulnerability?

- A. Session hijacking
- B. Cross-site request forgery (CSRF)
- C. Cross-Site Scripting (XSS)
- D. Command injection

Answer: C

NEW QUESTION 192

- (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 196

- (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 200

- (Exam Topic 15)

Which of the following is considered the FIRST step when designing an internal security control assessment?

- A. Create a plan based on recent vulnerability scans of the systems in question.
- B. Create a plan based on comprehensive knowledge of known breaches.
- C. Create a plan based on a recognized framework of known controls.
- D. Create a plan based on reconnaissance of the organization's infrastructure.

Answer: D

NEW QUESTION 205

- (Exam Topic 15)

Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

- A. Center for Internet Security (CIS)
- B. Common Vulnerabilities and Exposures (CVE)
- C. Open Web Application Security Project (OWASP)

D. Common Vulnerability Scoring System (CVSS)

Answer: D

NEW QUESTION 207

- (Exam Topic 15)

The Chief Information Security Officer (CISO) is concerned about business application availability. The organization was recently subject to a ransomware attack that resulted in the unavailability of applications and services for 10 working days that required paper-based running of all main business processes. There are now aggressive plans to enhance the Recovery Time Objective (RTO) and cater for more frequent data captures. Which of the following solutions should be implemented to fully comply to the new business requirements?

- A. Virtualization
- B. Antivirus
- C. Process isolation
- D. Host-based intrusion prevention system (HIPS)

Answer: A

NEW QUESTION 210

- (Exam Topic 15)

What requirement MUST be met during internal security audits to ensure that all information provided is expressed as an objective assessment without risk of retaliation?

- A. The auditor must be independent and report directly to the management.
- B. The auditor must utilize automated tools to back their findings.
- C. The auditor must work closely with both the information Technology (IT) and security sections of an organization.
- D. The auditor must perform manual reviews of systems and processes.

Answer: A

NEW QUESTION 211

- (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 212

- (Exam Topic 15)

According to the (ISC)? ethics canon "act honorably, honestly, justly, responsibly, and legally," which order should be used when resolving conflicts?

- A. Public safety and duties to principals, individuals, and the profession
- B. Individuals, the profession, and public safety and duties to principals
- C. Individuals, public safety and duties to principals, and the profession
- D. The profession, public safety and duties to principals, and individuals

Answer: A

NEW QUESTION 216

- (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 217

- (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 219

- (Exam Topic 15)

What is a risk of using commercial off-the-shelf (COTS) products?

- A. COTS products may not map directly to an organization's security requirements.
- B. COTS products are typically more expensive than developing software in-house.
- C. Cost to implement COTS products is difficult to predict.
- D. Vendors are often hesitant to share their source code.

Answer: A

NEW QUESTION 220

- (Exam Topic 15)

Which of the following types of hosts should be operating in the demilitarized zone (DMZ)?

- A. Hosts intended to provide limited access to public resources
- B. Database servers that can provide useful information to the public
- C. Hosts that store unimportant data such as demographical information
- D. File servers containing organizational data

Answer: A

NEW QUESTION 224

- (Exam Topic 15)

A software engineer uses automated tools to review application code and search for application flaws, back doors, or other malicious code. Which of the following is the FIRST Software Development Life Cycle (SDLC) phase where this takes place?

- A. Design
- B. Test
- C. Development
- D. Deployment

Answer: C

NEW QUESTION 229

- (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 230

- (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 234

- (Exam Topic 15)

When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

- A. Public safety, duties to individuals, duties to the profession, and duties to principals
- B. Public safety, duties to principals, duties to individuals, and duties to the profession
- C. Public safety, duties to the profession, duties to principals, and duties to individuals
- D. Public safety, duties to principals, duties to the profession, and duties to individuals

Answer: C

NEW QUESTION 235

- (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 240

- (Exam Topic 15)

The security team has been tasked with performing an interface test against a frontend external facing application and needs to verify that all input fields protect against invalid input. Which of the following BEST assists this process?

- A. Application fuzzing
- B. Instruction set simulation
- C. Regression testing
- D. Sanity testing

Answer: A

NEW QUESTION 243

- (Exam Topic 15)

An access control list (ACL) on a router is a feature MOST similar to which type of firewall?

- A. Packet filtering firewall
- B. Application gateway firewall
- C. Heuristic firewall
- D. Stateful firewall

Answer: B

NEW QUESTION 244

- (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 249

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 254

- (Exam Topic 15)

An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

- A. Engage a third-party auditing firm.
- B. Review security architecture.
- C. Perform incremental assessments.
- D. Conduct penetration testing.

Answer: C

NEW QUESTION 255

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 256

- (Exam Topic 15)

A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?

- A. Username and personal identification number (PIN)
- B. Fingerprint and retinal scanners
- C. Short Message Services (SMS) and smartphone authenticator
- D. Hardware token and password

Answer: D

NEW QUESTION 257

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 261

- (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 262

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 263

- (Exam Topic 15)

Which of the following documents specifies services from the client's viewpoint?

- A. Service level report
- B. Business impact analysis (BIA)
- C. Service level agreement (SLA)
- D. Service Level Requirement (SLR)

Answer: C

NEW QUESTION 267

- (Exam Topic 15)

How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?

- A. Access control can rely on the Operating System (OS), but eavesdropping is
- B. Access control cannot rely on the Operating System (OS), and eavesdropping
- C. Access control can rely on the Operating System (OS), and eavesdropping is
- D. Access control cannot rely on the Operating System (OS), and eavesdropping

Answer: C

NEW QUESTION 271

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 272

- (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 275

- (Exam Topic 15)

Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

- A. Public-Key Infrastructure (PKI)
- B. Symmetric key cryptography
- C. Digital signatures
- D. Biometric authentication

Answer: C

NEW QUESTION 279

- (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 281

- (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 286

- (Exam Topic 15)

An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

- A. The attacker could publicly share confidential comments found in the stolen code.
- B. Competitors might be able to steal the organization's ideas by looking at the stolen code.
- C. A competitor could run their own copy of the organization's website using the stolen code.
- D. Administrative credentials or keys hard-coded within the stolen code could be used to access sensitive data.

Answer: A

NEW QUESTION 290

- (Exam Topic 15)

Which of the following BEST describes the purpose of Border Gateway Protocol (BGP)?

- A. Maintain a list of network paths between internet routers.
- B. Provide Routing Information Protocol (RIP) version 2 advertisements to neighboring layer 3 devices.
- C. Provide firewall services to cloud-enabled applications.
- D. Maintain a list of efficient network paths between autonomous systems.

Answer: B

NEW QUESTION 291

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 293

- (Exam Topic 15)

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

- A. nslookup
- B. netstat -a
- C. ipconfig /a
- D. arp -a

Answer: B

NEW QUESTION 297

- (Exam Topic 15)

What is the PRIMARY objective of business continuity planning?

- A. Establishing a cost estimate for business continuity recovery operations
- B. Restoring computer systems to normal operations as soon as possible
- C. Strengthening the perceived importance of business continuity planning among senior management
- D. Ensuring timely recovery of mission-critical business processes

Answer: B

NEW QUESTION 302

- (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 304

- (Exam Topic 15)

An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

- A. nslookup
- B. show config
- C. netstat
- D. show interface
- E. show counters

Answer: D

NEW QUESTION 307

- (Exam Topic 15)

Which software defined networking (SDN) architectural component is responsible for translating network requirements?

- A. SDN Application
- B. SDN Data path
- C. SDN Controller
- D. SDN Northbound Interfaces

Answer: D

NEW QUESTION 310

- (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 315

- (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 319

- (Exam Topic 15)

Which of the following is considered the PRIMARY security issue associated with encrypted e-mail messages?

- A. Key distribution
- B. Storing attachments in centralized repositories
- C. Scanning for viruses and other malware
- D. Greater costs associated for backups and restores

Answer: C

NEW QUESTION 323

- (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 326

- (Exam Topic 15)

What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

- A. Contract negotiation
- B. Vendor demonstration
- C. Supplier request
- D. Business need

Answer: D

NEW QUESTION 331

- (Exam Topic 15)

A recent information security risk assessment identified weak system access controls on mobile devices as a high risk. 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 333

- (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 334

- (Exam Topic 15)

A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

- A. Validate passwords using a stored procedure.
- B. Allow only the application to have access to the password field in order to verify user authentication.

- C. Use a salted cryptographic hash of the password.
- D. Encrypt the entire database and embed an encryption key in the application.

Answer: C

NEW QUESTION 339

- (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 340

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 344

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 346

- (Exam Topic 15)

A firm within the defense industry has been directed to comply with contractual requirements for encryption of a government client's Controlled Unclassified Information (CUI). What encryption strategy represents how to protect data at rest in the MOST efficient and cost-effective manner?

- A. Perform physical separation of program information and encrypt only information deemed critical by the defense client
- B. Perform logical separation of program information, using virtualized storage solutions with built-in encryption at the virtualization layer
- C. Perform logical separation of program information, using virtualized storage solutions with encryption management in the back-end disk systems
- D. Implement data at rest encryption across the entire storage area network (SAN)

Answer: C

NEW QUESTION 350

- (Exam Topic 15)

What is considered a compensating control for not having electrical surge protectors installed?

- A. Having dual lines to network service providers built to the site
- B. Having backup diesel generators installed to the site
- C. Having a hot disaster recovery (DR) environment for the site
- D. Having network equipment in active-active clusters at the site

Answer: D

NEW QUESTION 353

- (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 357

- (Exam Topic 15)

A Certified Information Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC) Code of Professional Ethics, which of the following should the CISSP do?

- A. Review the CISSP guidelines for performing a vulnerability assessment before proceeding to complete it
- B. Review the PCI requirements before performing the vulnerability assessment
- C. Inform the CISO that they are unable to perform the task because they should render only those services for which they are fully competent and qualified
- D. Since they are CISSP certified, they have enough knowledge to assist with the request, but will need assistance in order to complete it in a timely manner

Answer: C

NEW QUESTION 362

- (Exam Topic 15)

The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

- A. Data loss protection (DLP)
- B. Intrusion detection
- C. Vulnerability scanner
- D. Information Technology Asset Management (ITAM)

Answer: D

NEW QUESTION 365

- (Exam Topic 15)

A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

- A. Hardware encryption
- B. Certificate revocation list (CRL) policy
- C. Trusted Platform Module (TPM)
- D. Key exchange

Answer: B

NEW QUESTION 368

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 373

- (Exam Topic 15)

An organization with divisions in the United States (US) and the United Kingdom (UK) processes data comprised of personal information belonging to subjects living in the European Union (EU) and in the US. Which data MUST be handled according to the privacy protections of General Data Protection Regulation (GDPR)?

- A. Only the EU citizens' data
- B. Only the EU residents' data
- C. Only the UK citizens' data
- D. Only data processed in the UK

Answer: A

NEW QUESTION 374

- (Exam Topic 15)

Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

- A. Instant messaging or chat applications
- B. E-mail applications
- C. Peer-to-Peer (P2P) file sharing applications
- D. End-to-end applications

Answer: A

NEW QUESTION 375

- (Exam Topic 15)

What industry-recognized document could be used as a baseline reference that is related to data security and business operations for conducting a security assessment?

- A. Service Organization Control (SOC) 1 Type 2
- B. Service Organization Control (SOC) 2 Type 1

- C. Service Organization Control (SOC) 1 Type 1
- D. Service Organization Control (SOC) 2 Type 2

Answer: D

NEW QUESTION 378

- (Exam Topic 15)

What is the PRIMARY reason that a bit-level copy is more desirable than a file-level copy when replicating a hard drive's contents for an e-discovery investigation?

- A. Files that have been deleted will be transferred.
- B. The file and directory structure is retained.
- C. File-level security settings will be preserved.
- D. The corruption of files is less likely.

Answer: A

NEW QUESTION 381

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 382

- (Exam Topic 15)

In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

- A. Increase logging levels.
- B. Implement bi-annual reviews.
- C. Create policies for system access.
- D. Implement and review risk-based alerts.

Answer: D

NEW QUESTION 385

- (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 386

- (Exam Topic 15)

Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages?

- A. Diffie-Hellman
- B. Digital Signature Algorithm (DSA)
- C. Rivest-Shamir-Adleman (RSA)
- D. Kerberos

Answer: C

NEW QUESTION 389

- (Exam Topic 15)

What is the BEST design for securing physical perimeter protection?

- A. Crime Prevention through Environmental Design (CPTED)
- B. Barriers, fences, gates, and walls
- C. Business continuity planning (BCP)
- D. Closed-circuit television (CCTV)

Answer: B

NEW QUESTION 391

- (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 392

- (Exam Topic 15)

Which of the following BEST describes when an organization should conduct a black box security audit on a new software product?

- A. When the organization wishes to check for non-functional compliance
- B. When the organization wants to enumerate known security vulnerabilities across their infrastructure
- C. When the organization has experienced a security incident
- D. When the organization is confident the final source code is complete

Answer: B

NEW QUESTION 393

- (Exam Topic 15)

An organization wants to migrate to Session Initiation Protocol (SIP) to save on telephony expenses. Which of the following security related statements should be considered in the decision-making process?

- A. Cloud telephony is less secure and more expensive than digital telephony services.
- B. SIP services are more secure when used with multi-layer security proxies.
- C. H.323 media gateways must be used to ensure end-to-end security tunnels.
- D. Given the behavior of SIP traffic, additional security controls would be required.

Answer: C

NEW QUESTION 395

- (Exam Topic 15)

An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

- A. The link is improperly terminated
- B. One of the devices is misconfigured
- C. The cable length is excessive.
- D. One of the devices has a hardware issue.

Answer: A

NEW QUESTION 396

- (Exam Topic 15)

Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

- A. Centralized network provisioning
- B. Centralized network administrator control
- C. Reduced network latency when scaled
- D. Reduced hardware footprint and cost

Answer: B

NEW QUESTION 401

- (Exam Topic 15)

Which media sanitization methods should be used for data with a high security categorization?

- A. Clear or destroy
- B. Clear or purge
- C. Destroy or delete
- D. Purge or destroy

Answer: D

NEW QUESTION 404

- (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 405

- (Exam Topic 15)

Which of the following is used to ensure that data mining activities Will NOT reveal sensitive data?

- A. Implement two-factor authentication on the underlying infrastructure.
- B. Encrypt data at the field level and tightly control encryption keys.
- C. Preprocess the databases to see if inn can be disclosed from the learned patterns.
- D. Implement the principle of least privilege on data elements so a reduced number of users can access the database.

Answer: D

NEW QUESTION 406

- (Exam Topic 15)

Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

- A. Payload encryption
- B. Sender confidentiality
- C. Sender non-repudiation
- D. Multi-factor authentication (MFA)

Answer: C

NEW QUESTION 407

- (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 408

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 411

- (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 416

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 420

- (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 421

- (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 422

- (Exam Topic 15)

During testing, where are the requirements to inform parent organizations, law enforcement, and a computer incident response team documented?

- A. Unit test results
- B. Security assessment plan
- C. System integration plan
- D. Security Assessment Report (SAR)

Answer: D

NEW QUESTION 423

- (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 424

- (Exam Topic 15)

Which of the following is a covert channel type?

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

Answer: A

NEW QUESTION 426

- (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 429

- (Exam Topic 15)

The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in which role in order to ensure proper protection of data during and after the cloud migration?

- A. Information owner
- B. General Counsel
- C. Chief Information Security Officer (CISO)
- D. Chief Security Officer (CSO)

Answer: A

NEW QUESTION 430

- (Exam Topic 15)

A hospital's building controls system monitors and operates the environmental equipment to maintain a safe and comfortable environment. Which of the following could be

used to minimize the risk of utility supply interruption?

- A. Digital devices that can turn equipment off and continuously cycle rapidly in order to increase supplies and conceal activity on the hospital network
- B. Standardized building controls system software with high connectivity to hospital networks
- C. Lock out maintenance personnel from the building controls system access that can impact critical utility supplies
- D. Digital protection and control devices capable of minimizing the adverse impact to critical utility

Answer: D

NEW QUESTION 435

- (Exam Topic 15)

What is the MOST common cause of Remote Desktop Protocol (RDP) compromise?

- A. Port scan
- B. Brute force attack
- C. Remote exploit
- D. Social engineering

Answer: B

NEW QUESTION 440

- (Exam Topic 15)

A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

- A. Network is flooded with communication traffic by the attacker.
- B. Organization loses control of their network devices.
- C. Network management communications is disrupted.
- D. Attacker accesses sensitive information regarding the network topology.

Answer: B

NEW QUESTION 443

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 445

- (Exam Topic 15)

In Federated Identity Management (FIM), which of the following represents the concept of federation?

- A. Collection of information logically grouped into a single entity
- B. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications
- C. Collection of information for common identities in a system
- D. Collection of domains that have established trust among themselves

Answer: D

NEW QUESTION 450

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 453

- (Exam Topic 15)

Which of the following techniques evaluates the secure design principles of network OF software architectures?

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

Answer: B

NEW QUESTION 458

- (Exam Topic 15)

What should be used to determine the risks associated with using Software as a Service (SaaS) for collaboration and email?

- A. Cloud access security broker (CASB)
- B. Open Web Application Security Project (OWASP)
- C. Process for Attack Simulation and Threat Analysis (PASTA)
- D. Common Security Framework (CSF)

Answer: A

NEW QUESTION 463

- (Exam Topic 15)

How does Radio-Frequency Identification (RFID) assist with asset management?

- A. It uses biometric information for system identification.
- B. It uses two-factor authentication (2FA) for system identification.
- C. It transmits unique Media Access Control (MAC) addresses wirelessly.
- D. It transmits unique serial numbers wirelessly.

Answer: B

NEW QUESTION 468

- (Exam Topic 15)

Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

- A. The business owner
- B. security subject matter expert (SME)
- C. The application owner
- D. A developer subject matter expert (SME)

Answer: B

NEW QUESTION 471

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

Answer: D

NEW QUESTION 472

- (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 475

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 476

- (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 480

- (Exam Topic 15)

Which of the following are all elements of a disaster recovery plan (DRP)?

- A. Document the actual location of the ORP, developing an incident notification procedure, evaluating costs of critical components
- B. Document the actual location of the ORP, developing an incident notification procedure, establishing recovery locations
- C. Maintain proper documentation of all server logs, developing an incident notification procedure, establishing recovery locations
- D. Document the actual location of the ORP, recording minutes at all ORP planning sessions, establishing recovery locations

Answer: C

NEW QUESTION 483

- (Exam Topic 14)

Which of the following is the BEST technique to facilitate secure software development?

- A. Adhere to secure coding practices for the software application under development.
- B. Conduct penetrating testing for the software application under development.
- C. Develop a threat modeling review for the software application under development.
- D. Perform a code review process for the software application under development.

Answer: A

NEW QUESTION 485

- (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 490

- (Exam Topic 15)

A security professional has been requested by the Board of Directors and Chief Information Security Officer (CISO) to perform an internal and external penetration test. What is the BEST course of action?

- A. Review data localization requirements and regulations.
- B. Review corporate security policies and procedures,
- C. With notice to the Configuring a Wireless Access Point (WAP) with the same Service Set Identifier external test.
- D. With notice to the organization, perform an external penetration test first, then an internal test.

Answer: D

NEW QUESTION 491

- (Exam Topic 15)

Building blocks for software-defined networks (SDN) require which of the following?

- A. The SDN is mostly composed of virtual machines (VM).
- B. The SDN is composed entirely of client-server pairs.
- C. Virtual memory is used in preference to random-access memory (RAM).
- D. Random-access memory (RAM) is used in preference to virtual memory.

Answer: C

NEW QUESTION 495

- (Exam Topic 14)

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

- A. Service provider(s) utilized by the organization
- B. Whether it will impact personal use
- C. Number of mobile users in the organization
- D. Feasibility of downloads due to available bandwidth

Answer: C

NEW QUESTION 499

- (Exam Topic 14)

What form of attack could this represent?

- A. A Denial of Service (DoS) attack against the gateway router because the router can no longer accept packets from
- B. A transport layer attack that prevents the resolution of 10.102.10.6 address
- C. A Denial of Service (DoS) attack against 10.102.10.2 because it cannot respond correctly to ARP requests
- D. A masquerading attack that sends packets intended for 10.102.10.6 to 10.102.10.2

Answer: D

NEW QUESTION 501

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 503

- (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 504

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 507

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 508

- (Exam Topic 14)

When developing the entitlement review process, which of the following roles is responsible for determining who has a need for the information?

- A. Data Custodian
- B. Data Owner
- C. Database Administrator
- D. Information Technology (IT) Director

Answer: B

NEW QUESTION 512

- (Exam Topic 14)

What should an auditor do when conducting a periodic audit on media retention?

- A. Check electronic storage media to ensure records are not retained past their destruction date.
- B. Ensure authorized personnel are in possession of paper copies containing Personally Identifiable Information....
- C. Check that hard disks containing backup data that are still within a retention cycle are being destroyed....
- D. Ensure that data shared with outside organizations is no longer on a retention schedule.

Answer: A

NEW QUESTION 516

- (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 519

- (Exam Topic 14)

What type of access control determines the authorization to resource based on pre-defined job titles within an organization?

- A. Role-Based Access Control (RBAC)
- B. Role-based access control
- C. Non-discretionary access control
- D. Discretionary Access Control (DAC)

Answer: A

NEW QUESTION 523

- (Exam Topic 14)

An organization is considering outsourcing applications and data to a Cloud Service Provider (CSP). Which of the following is the MOST important concern regarding privacy?

- A. The CSP determines data criticality.
- B. The CSP provides end-to-end encryption services.
- C. The CSP's privacy policy may be developed by the organization.
- D. The CSP may not be subject to the organization's country legislation.

Answer: D

NEW QUESTION 527

- (Exam Topic 14)

An organization has implemented a new backup process which protects confidential data by encrypting the information stored on backup tapes. Which of the following is a MAJOR data confidentiality concern after the implementation of this new backup process?

- A. Tape backup rotation
- B. Pre-existing backup tapes
- C. Tape backup compression
- D. Backup tape storage location

Answer: D

NEW QUESTION 532

- (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 537

- (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 540

- (Exam Topic 14)

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

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

Answer: D

Explanation:

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

NEW QUESTION 541

- (Exam Topic 14)

Which of the following is a characteristic of the independent testing of a program?

- A. Independent testing increases the likelihood that a test will expose the effect of a hidden feature.
- B. Independent testing decreases the likelihood that a test will expose the effect of a hidden feature.
- C. Independent testing teams help decrease the cost of creating test data and system design specification.
- D. Independent testing teams help identify functional requirements and Service Level Agreements (SLA)

Answer: A

NEW QUESTION 544

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 545

- (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 546

- (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 551

- (Exam Topic 14)

The Secure Shell (SSH) version 2 protocol supports.

- A. availability, accountability, compression, and integrity,
- B. authentication, availability, confidentiality, and integrity.
- C. accountability, compression, confidentiality, and integrity.
- D. authentication, compression, confidentiality, and integrity.

Answer: D

NEW QUESTION 555

- (Exam Topic 14)

Which of the following is a MAJOR concern when there is a need to preserve or retain information for future retrieval?

- A. Laws and regulations may change in the interim, making it unnecessary to retain the information.
- B. The expense of retaining the information could become untenable for the organization.
- C. The organization may lose track of the information and not dispose of it securely.
- D. The technology needed to retrieve the information may not be available in the future.

Answer: C

NEW QUESTION 556

- (Exam Topic 14)

- A. Verify the camera's log for recent logins outside of the Internet Technology (IT) department.
- B. Verify the security and encryption protocol the camera uses.
- C. Verify the security camera requires authentication to log into the management console.
- D. Verify the most recent firmware version is installed on the camera.

Answer: D

NEW QUESTION 560

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 564

- (Exam Topic 14)

Compared with hardware cryptography, software cryptography is generally

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

Answer: A

Explanation:

Reference:

<https://www.ontrack.com/uk/blog/making-data-simple/hardware-encryption-vs-software-encryption-the-simple>

NEW QUESTION 568

- (Exam Topic 14)

How can an attacker exploit overflow to execute arbitrary code?

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

Answer: A

NEW QUESTION 571

- (Exam Topic 14)

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

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

Answer: C

Explanation:

Reference: <https://books.google.com.pk/books?id=LnjxBwAAQBAJ&pg=PT504&lpg=PT504&dq=CISSP+mechanism+us>

NEW QUESTION 572

- (Exam Topic 14)

Which of the following is a method of attacking internet (IP) v6 Layer 3 and Layer 4 ?

- A. Synchronize sequence numbers (SVN) flooding
- B. Internet Control Message Protocol (IOP) flooring
- C. Domain Name Server [DNS] cache poisoning
- D. Media Access Control (MAC) flooding

Answer: A

NEW QUESTION 576

- (Exam Topic 14)

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

- A. To document those who were In possession of the evidence at every point In time
- B. To collect records of all digital forensic professionals working on a case
- C. To document collected digital evidence
- D. To ensure that digital evidence is not overlooked during the analysis

Answer: A

NEW QUESTION 579

- (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 580

- (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 584

- (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 586

- (Exam Topic 14)

Which of the following is used to detect steganography?

- A. Audio analysis
- B. Statistical analysis
- C. Reverse engineering
- D. Cryptanalysis

Answer: C

NEW QUESTION 590

- (Exam Topic 14)

Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

- A. An attack which forces an end user to execute unwanted actions on a web application in which they are currently authenticated
- B. An attack that injects a script into a web page to execute a privileged command
- C. An attack that makes an illegal request across security zones and thereby forges itself into the security database of the system
- D. An attack that forges a false Structure Query Language (SQL) command across systems

Answer: A

Explanation:

Reference: <https://portswigger.net/web-security/csrf>

NEW QUESTION 595

- (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)

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

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

Answer: B

NEW QUESTION 604

- (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 606

- (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 610

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 615

- (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)

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

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

Answer: C

NEW QUESTION 619

- (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 624

- (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 627

- (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)

What is the MOST effective way to protect privacy?

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

Answer: D

NEW QUESTION 632

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 635

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 639

- (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. In incremental data backup must be done after each system change.

Answer: D

NEW QUESTION 642

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 643

- (Exam Topic 14)

Which open standard could I large corporation deploy for authorization services for single sign-on (SSO) use across multiple internal and external application?

- A. Terminal Access Controller Access Control System (TACACS)
- B. Security Assertion Markup Language (SAML)
- C. Lightweight Directory Access Protocol (LDAP)
- D. Active Directory Federation Services (ADFS)

Answer: B

NEW QUESTION 648

- (Exam Topic 14)

Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

- A. Test
- B. Assessment
- C. Review
- D. Peer review

Answer: C

Explanation:

Reference: <https://books.google.com.pk/books?id=W2TvAgAAQBAJ&pg=PA256&lpg=PA256&dq=process+in+the+acce>

NEW QUESTION 650

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 654

- (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 658

- (Exam Topic 14)

A vehicle of a private courier company that transports backup data for offsite storage was robbed while in transport backup data for offsite was robbed while in transit. The incident management team is now responsible to estimate the robbery, which of the following would help the incident management team to MOST effectively analyze the business impact of the robbery?

- A. Log of backup administrative actions
- B. Log of the transported media and its classification marking
- C. Log of the transported media and Its detailed contents
- D. Log of backed up data and their respective data custodians

Answer: B

NEW QUESTION 660

- (Exam Topic 14)

According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

- A. Level 0: Incomplete
- B. Level 1: Performed
- C. Level 2: Managed
- D. Level 3: Defined

Answer: D

NEW QUESTION 664

- (Exam Topic 14)

The MAIN task of promoting security for Personal Computers (PC) is

- A. understanding the technical controls and ensuring they are correctly installed.
- B. understanding the required systems and patching processes for different Operating Systems (OS).
- C. making sure that users are using only valid, authorized software, so that the chance of virus infection
- D. making users understand the risks to the machines and data, so they will take appropriate steps to protect them.

Answer: C

NEW QUESTION 665

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 669

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 674

- (Exam Topic 14)

Which of the following is MOST critical in a contract for data disposal on a hard drive with a third party?

- A. Authorized destruction times
- B. Allowed unallocated disk space
- C. Amount of overwrites required
- D. Frequency of recovered media

Answer: C

NEW QUESTION 677

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 682

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 684

- (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 685

- (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 688

- (Exam Topic 14)

What is the MAIN reason to ensure the appropriate retention periods are enforced for data stored on electronic media?

- A. To reduce the carbon footprint by eliminating paper
- B. To create an inventory of data assets stored on disk for backup and recovery
- C. To declassify information that has been improperly classified
- D. To reduce the risk of loss, unauthorized access, use, modification, and disclosure

Answer: D

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 690

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 695

- (Exam Topic 14)

Which of the following provides the GREATEST level of data security for a Virtual Private Network (VPN) connection?

- A. Internet Protocol Payload Compression (IPComp)
- B. Internet Protocol Security (IPSec)
- C. Extensible Authentication Protocol (EAP)
- D. Remote Authentication Dial-In User Service (RADIUS)

Answer: B

NEW QUESTION 698

- (Exam Topic 14)

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

- A. Directive
- B. Detective

- C. Corrective
- D. Preventative

Answer: A

Explanation:

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

NEW QUESTION 699

- (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 701

- (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	Assurance Level
Structurally tested	1
Methodically tested and checked	2
Methodically designed, tested, and reviewed	3
Functionally tested	4
Semiformally verified design and tested	5
Formally verified design and tested	6
Semiformally designed and tested	7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Level of Evaluation	Assurance Level
Structurally tested	Functionally tested 1
Methodically tested and checked	Structurally tested 2
Methodically designed, tested, and reviewed	Methodically tested and checked 3
Functionally tested	Methodically designed, tested, and reviewed 4
Semiformally verified design and tested	Semiformally designed and tested 5
Formally verified design and tested	Semiformally verified design and tested 6
Semiformally designed and tested	Formally verified design and tested 7

NEW QUESTION 703

- (Exam Topic 14)

Organization A is adding a large collection of confidential data records that it received when it acquired Organization B to its data store. Many of the users and staff from Organization B are no longer available. Which of the following MUST Organization A do to properly classify and secure the acquired data?

- A. Assign data owners from Organization A to the acquired data.
- B. Create placeholder accounts that represent former users from Organization B.
- C. Archive audit records that refer to users from Organization A.
- D. Change the data classification for data acquired from Organization B.

Answer: A

NEW QUESTION 706

- (Exam Topic 14)

An audit of an application reveals that the current configuration does not match the configuration of the originally implemented application. Which of the following is the FIRST action to be taken?

- A. Recommend an update to the change control process.
- B. Verify the approval of the configuration change.
- C. Roll back the application to the original configuration.
- D. Document the changes to the configuration.

Answer: B

NEW QUESTION 709

- (Exam Topic 14)

Information security metrics provide the GREATEST value to management when based upon the security manager's knowledge of which of the following?

- A. Likelihood of a security breach
- B. Value of information assets
- C. Cost of implementing effective controls
- D. Benefits related to quantitative analysts

Answer: B

NEW QUESTION 712

- (Exam Topic 14)

A security professional recommends that a company integrate threat modeling into its Agile development processes. Which of the following BEST describes the benefits of this approach?

- A. Reduce application development costs.
- B. Potential threats are addressed later in the Software Development Life Cycle (SDLC).
- C. Improve user acceptance of implemented security controls.
- D. Potential threats are addressed earlier in the Software Development Life Cycle (SDLC).

Answer: D

NEW QUESTION 715

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 716

- (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 transaction parties.
- C. They verify the transaction parties' private keys.
- D. They provide a secure communication channel to the transaction parties.

Answer: D

NEW QUESTION 719

- (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 724

- (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 727

- (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 728

- (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 733

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 738

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 743

- (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 748

- (Exam Topic 14)

A security consultant has been hired by a company to establish its vulnerability management program. The consultant is now in the deployment phase. Which of the following tasks is part of this process?

- A. Select and procure supporting technologies.

- B. Determine a budget and cost analysis for the program.
- C. Measure effectiveness of the program's stated goals.
- D. Educate and train key stakeholders.

Answer: C

NEW QUESTION 751

- (Exam Topic 14)

Which of the following MOST applies to session initiation protocol (SIP) security?

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

Answer: C

NEW QUESTION 755

- (Exam Topic 14)

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

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

Answer: A

Explanation:

Reference: <https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA478&lpg=PA478&dq=CISSP+taken+into+acc>

NEW QUESTION 756

- (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 760

- (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 765

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 767

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 769

- (Exam Topic 14)

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

- A. Move ahead with the acquisition process, and purchase the flagship software
- B. Conduct a security review of the OS
- C. Perform functionality testing
- D. Enter into contract negotiations ensuring Service Level Agreements (SLA) are established to include security patching

Answer: B

NEW QUESTION 771

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)