

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

<https://www.2passeasy.com/dumps/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)

An organization plans to acquire @ commercial off-the-shelf (COTS) system to replace their aging home-built reporting system. When should the organization's security team FIRST get involved in this acquisition's life cycle?

- A. When the system is being designed, purchased, programmed, developed, or otherwise constructed
- B. When the system is verified and validated
- C. When the system is deployed into production
- D. When the need for a system is expressed and the purpose of the system is documented

Answer: D

NEW QUESTION 3

- (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 4

- (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 5

- (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 6

- (Exam Topic 15)

An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration test is needed?

- A. Functional test
- B. Unit test
- C. Grey box
- D. White box

Answer: C

NEW QUESTION 7

- (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 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)

The security architect is designing and implementing an internal certification authority to generate digital certificates for all employees. Which of the following is the BEST solution to securely store the private keys?

- A. Physically secured storage device
- B. Encrypted flash drive
- C. Public key infrastructure (PKI)
- D. Trusted Platform Module (TPM)

Answer: C

NEW QUESTION 10

- (Exam Topic 15)

Which of the following access control models is MOST restrictive?

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

Answer: B

NEW QUESTION 11

- (Exam Topic 15)

An organization has implemented a password complexity and an account lockout policy enforcing five incorrect logins tries within ten minutes. Network users have reported significantly increased account lockouts. Which of the following security principles is this company affecting?

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

Answer: A

NEW QUESTION 12

- (Exam Topic 15)

Which of the following routing protocols is used to exchange route information between public autonomous systems?

- A. OSPF
- B. BGP
- C. EIGRP
- D. RIP

Answer: B

NEW QUESTION 15

- (Exam Topic 15)

Which of the following provides the MOST secure method for Network Access Control (NAC)?

- A. Media Access Control (MAC) filtering
- B. 802.1X authentication
- C. Application layer filtering
- D. Network Address Translation (NAT)

Answer: B

NEW QUESTION 19

- (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 24

- (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 29

- (Exam Topic 15)

To minimize the vulnerabilities of a web-based application, which of the following FIRST actions will lock down the system and minimize the risk of an attack?

- A. Install an antivirus on the server
- B. Run a vulnerability scanner
- C. Review access controls
- D. Apply the latest vendor patches and updates

Answer: D

NEW QUESTION 31

- (Exam Topic 15)

Which of the following is a common term for log reviews, synthetic transactions, and code reviews?

- A. Security control testing
- B. Application development
- C. Spiral development functional testing
- D. DevOps Integrated Product Team (IPT) development

Answer: B

NEW QUESTION 35

- (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 38

- (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 40

- (Exam Topic 15)

Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

- A. Application threat modeling
- B. Secure software development.
- C. Agile software development
- D. Penetration testing

Answer: A

NEW QUESTION 44

- (Exam Topic 15)

An organization needs a general purpose document to prove that its internal controls properly address security, availability, processing integrity, confidentiality or privacy risks. Which of the following reports is required?

- A. A Service Organization Control (SOC) 3 report
- B. The Statement on Standards for Attestation Engagements N
- C. 18 (SSAE 18)
- D. A Service Organization Control (SOC) 2 report
- E. The International Organization for Standardization (ISO) 27001

Answer: C

NEW QUESTION 46

- (Exam Topic 15)

Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

- A. Employee evaluation of the training program
- B. Internal assessment of the training program's effectiveness
- C. Multiple choice tests to participants
- D. Management control of reviews

Answer: B

NEW QUESTION 49

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 50

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 53

- (Exam Topic 15)

Which of the following uses the destination IP address to forward packets?

- A. A bridge
- B. A Layer 2 switch
- C. A router
- D. A repeater

Answer: C

NEW QUESTION 55

- (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 58

- (Exam Topic 15)

What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

- A. RAID-0
- B. RAID-1
- C. RAID-5
- D. RAID-6

Answer: A

NEW QUESTION 60

- (Exam Topic 15)

What method could be used to prevent passive attacks against secure voice communications between an organization and its vendor?

- A. Encryption in transit
- B. Configure a virtual private network (VPN)
- C. Configure a dedicated connection
- D. Encryption at rest

Answer: A

NEW QUESTION 62

- (Exam Topic 15)

Which of the following is the BEST way to mitigate circumvention of access controls?

- A. Multi-layer access controls working in isolation
- B. Multi-vendor approach to technology implementation
- C. Multi-layer firewall architecture with Internet Protocol (IP) filtering enabled
- D. Multi-layer access controls with diversification of technologies

Answer: D

NEW QUESTION 67

- (Exam Topic 15)

Which of the following is an indicator that a company's new user security awareness training module has been effective?

- A. There are more secure connections to the internal database servers.
- B. More incidents of phishing attempts are being reported.
- C. There are more secure connections to internal e-mail servers.
- D. Fewer incidents of phishing attempts are being reported.

Answer: B

NEW QUESTION 72

- (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 73

- (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 76

- (Exam Topic 15)

Which element of software supply chain management has the GREATEST security risk to organizations?

- A. New software development skills are hard to acquire.
- B. Unsupported libraries are often used.
- C. Applications with multiple contributors are difficult to evaluate.
- D. Vulnerabilities are difficult to detect.

Answer: B

NEW QUESTION 77

- (Exam Topic 15)

A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

SSID	Signal (RSSI)	Channel
Corporate	-50	9
Corporate	-69	10
Corporate	-67	11
Corporate	-63	6

Which of the following is MOST likely the cause of the issue?

- A. Channel overlap
- B. Poor signal
- C. Incorrect power settings
- D. Wrong antenna type

Answer: A

NEW QUESTION 82

- (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 87

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 88

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 91

- (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 93

- (Exam Topic 15)

A financial services organization has employed a security consultant to review processes used by employees across various teams. The consultant interviewed a member of the application development practice and found gaps in their threat model. Which of the following correctly represents a trigger for when a threat model should be revised?

- A. A new data repository is added.
- B. is After operating system (OS) patches are applied
- C. After a modification to the firewall rule policy
- D. A new developer is hired into the team.

Answer: D

NEW QUESTION 98

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 103

- (Exam Topic 15)

When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

- A. Assessing the Uniform Resource Locator (URL)
- B. Ensuring Secure Sockets Layer (SSL) certificates are signed by a certificate authority
- C. Ensuring that input validation is enforced
- D. Ensuring Secure Sockets Layer (SSL) certificates are internally signed

Answer: B

NEW QUESTION 104

- (Exam Topic 15)

What is the correct order of execution for security architecture?

- A. Governance, strategy and program management, project delivery, operations
- B. Strategy and program management, governance, project delivery, operations
- C. Governance, strategy and program management, operations, project delivery
- D. Strategy and program management, project delivery, governance, operations

Answer: A

NEW QUESTION 109

- (Exam Topic 15)

When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

- A. EAP-Transport Layer Security (TLS)
- B. EAP-Flexible Authentication via Secure Tunneling
- C. EAP-Tunneled Transport Layer Security (TLS)
- D. EAP-Protected Extensible Authentication Protocol (PEAP)

Answer: C

NEW QUESTION 111

- (Exam Topic 15)

A developer begins employment with an information technology (IT) organization. On the first day, the developer works through the list of assigned projects and finds that some files within those projects aren't accessible, Other developers working on the same project have no trouble locating and working on the. What is the MOST likely explanation for the discrepancy in access?

- A. The IT administrator had failed to grant the developer privileged access to the servers.
- B. The project files were inadvertently deleted.
- C. The new developer's computer had not been added to an access control list (ACL).
- D. The new developer's user account was not associated with the right roles needed for the projects.

Answer: A

NEW QUESTION 115

- (Exam Topic 15)

What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

- A. Capturing an image of the system
- B. Maintaining the chain of custody

- C. Complying with the organization's security policy
- D. Outlining all actions taken during the investigation

Answer: A

NEW QUESTION 117

- (Exam Topic 15)

Information Security Continuous Monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

- A. Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- B. Conduct a vulnerability assessment to discover current threats against the environment and incorporate them into the program.
- C. Respond to findings with technical management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- D. Analyze the data collected and report findings, determining the appropriate responses
- E. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

Answer: A

NEW QUESTION 120

- (Exam Topic 15)

Which of the following BEST represents a defense in depth concept?

- A. Network-based data loss prevention (DLP), Network Access Control (NAC), network-based Intrusion prevention system (NIPS), Port security on core switches
- B. Host-based data loss prevention (DLP), Endpoint anti-malware solution, Host-based integrity checker, Laptop locks, hard disk drive (HDD) encryption
- C. Endpoint security management, network intrusion detection system (NIDS), Network Access Control (NAC), Privileged Access Management (PAM), security information and event management (SIEM)
- D. Web application firewall (WAF), Gateway network device tuning, Database firewall, Next-Generation Firewall (NGFW), Tier-2 demilitarized zone (DMZ) tuning

Answer: C

NEW QUESTION 123

- (Exam Topic 15)

A software development company has a short timeline in which to deliver a software product. The software development team decides to use open-source software libraries to reduce the development time. What concept should software developers consider when using open-source software libraries?

- A. Open source libraries contain known vulnerabilities, and adversaries regularly exploit those vulnerabilities in the wild.
- B. Open source libraries can be used by everyone, and there is a common understanding that the vulnerabilities in these libraries will not be exploited.
- C. Open source libraries are constantly updated, making it unlikely that a vulnerability exists for an adversary to exploit.
- D. Open source libraries contain unknown vulnerabilities, so they should not be used.

Answer: A

NEW QUESTION 127

- (Exam Topic 15)

Which of the following criteria ensures information is protected relative to its importance to the organization?

- A. The value of the data to the organization's senior management
- B. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification
- C. Legal requirements determined by the organization headquarters' location
- D. Organizational stakeholders, with classification approved by the management board

Answer: D

NEW QUESTION 131

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 132

- (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 137

- (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 142

- (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 146

- (Exam Topic 15)

A security professional should ensure that clients support which secondary algorithm for digital signatures when a Secure Multipurpose Internet Mail Extension (S/MIME) is used?

- A. Triple Data Encryption Standard (3DES)
- B. Advanced Encryption Standard (AES)
- C. Digital Signature Algorithm (DSA)
- D. Rivest-Shamir-Adieman (RSA)

Answer: C

NEW QUESTION 148

- (Exam Topic 15)

Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

- A. To provide each manager with precise direction on selecting an appropriate recovery alternative
- B. To demonstrate to the regulatory bodies that the company takes business continuity seriously
- C. To demonstrate to the board of directors that senior management is committed to continuity recovery efforts
- D. To provide a formal declaration from senior management as required by internal audit to demonstrate sound business practices

Answer: D

NEW QUESTION 153

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 154

- (Exam Topic 15)

Which of the following is the MOST secure password technique?

- A. Passphrase
- B. One-time password
- C. Cognitive password
- D. dphertext

Answer: A

NEW QUESTION 159

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 160

- (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 161

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 163

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 166

- (Exam Topic 15)

Which of the following will accomplish Multi-Factor Authentication (MFA)?

- A. Issuing a smart card with a user-selected Personal Identification Number (PIN)
- B. Requiring users to enter a Personal Identification Number (PIN) and a password
- C. Performing a palm and retinal scan
- D. Issuing a smart card and a One Time Password (OTP) token

Answer: A

NEW QUESTION 170

- (Exam Topic 15)

A small office is running WiFi 4 APs, and neighboring offices do not want to increase the throughput to associated devices. Which of the following is the MOST cost-efficient way for the office to increase network performance?

- A. Add another AP.
- B. Disable the 2.4GHz radios
- C. Enable channel bonding.
- D. Upgrade to WiFi 5.

Answer: C

NEW QUESTION 174

- (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 175

- (Exam Topic 15)

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

- A. Security orchestration automation and response

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

Answer: A

NEW QUESTION 179

- (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 180

- (Exam Topic 15)

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

- A. Strict integration of application management, configuration management (CM), and phone management
- B. Management application installed on user phones that tracks all application events and cellular traffic
- C. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity
- D. Routine reports generated by the user's cellular phone provider that detail security events

Answer: B

NEW QUESTION 183

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 186

- (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 190

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 195

- (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 196

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 201

- (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 203

- (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 207

- (Exam Topic 15)

When defining a set of security controls to mitigate a risk, which of the following actions MUST occur?

- A. Each control's effectiveness must be evaluated individually.
- B. Each control must completely mitigate the risk.
- C. The control set must adequately mitigate the risk.
- D. The control set must evenly divided the risk.

Answer: A

NEW QUESTION 212

- (Exam Topic 15)

Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

- A. Lower costs throughout the System Development Life Cycle (SDLC)
- B. Facilitate a root cause analysis (RCA)
- C. Enable generation of corrective action reports
- D. Avoid lengthy audit reports

Answer: B

NEW QUESTION 215

- (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 216

- (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 220

- (Exam Topic 15)

An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is MOST critical in creating acceptance tests or acceptance criteria for each release?

- A. Project managers
- B. Software developers
- C. Independent testers
- D. Business customers

Answer: D

NEW QUESTION 223

- (Exam Topic 15)

What documentation is produced FIRST when performing an effective physical loss control process?

- A. Deterrent controls list
- B. Security standards list
- C. inventory list
- D. Asset valuation list

Answer: C

NEW QUESTION 227

- (Exam Topic 15)

Which of the following is the PRIMARY goal of logical access controls?

- A. Restrict access to an information asset.
- B. Ensure integrity of an information asset.
- C. Restrict physical access to an information asset.
- D. Ensure availability of an information asset.

Answer: C

NEW QUESTION 230

- (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 233

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 237

- (Exam Topic 15)

Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

- A. Multiprotocol Label Switching (MPLS)
- B. Synchronous Optical Networking (SONET)
- C. Session Initiation Protocol (SIP)
- D. Fiber Channel Over Ethernet (FCoE)

Answer: A

NEW QUESTION 242

- (Exam Topic 15)

Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

- A. Quality design principles to ensure quality by design
- B. Policies to validate organization rules
- C. Cyber hygiene to ensure organizations can keep systems healthy
- D. Strong operational security to keep unit members safe

Answer: B

NEW QUESTION 247

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 249

- (Exam Topic 15)

Which of the following explains why classifying data is an important step in performing a Risk assessment?

- A. To provide a framework for developing good security metrics
- B. To justify the selection of costly security controls
- C. To classify the security controls sensitivity that helps scope the risk assessment
- D. To help determine the appropriate level of data security controls

Answer: D

NEW QUESTION 254

- (Exam Topic 15)

An organization's internal audit team performed a security audit on the company's system and reported that the manufacturing application is rarely updated along with other issues categorized as minor. Six months later, an external audit team reviewed the same system with the same scope, but identified severe weaknesses in the manufacturing application's security controls. What is MOST likely to be the root cause of the internal audit team's failure in detecting these security issues?

- A. Inadequate test coverage analysis
- B. Inadequate security patch testing
- C. Inadequate log reviews
- D. Inadequate change control procedures

Answer: A

NEW QUESTION 255

- (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 256

- (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 259

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 260

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 263

- (Exam Topic 15)

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

- A. iSCSI
- B. FCoE
- C. Three-tiered network
- D. Spine and leafE Top-of-rack switching

Answer: B

NEW QUESTION 265

- (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 270

- (Exam Topic 15)

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

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

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

Answer: B

NEW QUESTION 274

- (Exam Topic 15)

Upon commencement of an audit within an organization, which of the following actions is MOST important for the auditor(s) to take?

- A. Understand circumstances which may delay the overall audit timelines.
- B. Review all prior audit results to remove all areas of potential concern from the audit scope.
- C. Meet with stakeholders to review methodology, people to be interviewed, and audit scope.
- D. Meet with stakeholders to understand which types of audits have been completed.

Answer: C

NEW QUESTION 278

- (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 280

- (Exam Topic 15)

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

- A. Change driver
- B. Change implementer
- C. Program sponsor
- D. Project manager

Answer: D

NEW QUESTION 283

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 284

- (Exam Topic 15)

Which of the following factors is a PRIMARY reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy?

- A. Testing and Evaluation (TE) personnel changes
- B. Changes to core missions or business processes
- C. Increased Cross-Site Request Forgery (CSRF) attacks
- D. Changes in Service Organization Control (SOC) 2 reporting requirements

Answer: B

NEW QUESTION 286

- (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 287

- (Exam Topic 15)

Which of the following is the MOST appropriate technique for destroying magnetic platter style hard disk drives (HDD) containing data with a "HIGH" security categorization?

- A. Drill through the device and platters.
- B. Mechanically shred the entire HDD.
- C. Remove the control electronics.
- D. HP iProcess the HDD through a degaussing device.

Answer: D

NEW QUESTION 291

- (Exam Topic 15)

The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the foresight to enable what feature on all endpoints?

- A. Process isolation
- B. Trusted Platform Module (TPM)
- C. Address Space Layout Randomization (ASLR)
- D. Virtualization

Answer: C

NEW QUESTION 293

- (Exam Topic 15)

An organization is implementing data encryption using symmetric ciphers and the Chief Information Officer (CIO) is concerned about the risk of using one key to protect all sensitive data. The security practitioner has been tasked with recommending a solution to address the CIO's concerns. Which of the following is the BEST approach to achieving the objective by encrypting all sensitive data?

- A. Use a Secure Hash Algorithm 256 (SHA-256).
- B. Use a hierarchy of encryption keys.
- C. Use Hash Message Authentication Code (HMAC) keys.
- D. Use Rivest-Shamir-Adleman (RSA) keys.

Answer: D

NEW QUESTION 296

- (Exam Topic 15)

When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of

big data?

- A. Consolidated data collection
- B. Distributed storage locations
- C. Distributed data collection
- D. Centralized processing location

Answer: C

NEW QUESTION 298

- (Exam Topic 15)

Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

- A. Layer 3 switch
- B. VPN headend
- C. Next-generation firewall
- D. Proxy server
- E. Intrusion prevention

Answer: C

NEW QUESTION 300

- (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 302

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 304

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 307

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 312

- (Exam Topic 15)

Which of the following is the PRIMARY type of cryptography required to support non-repudiation of a digitally signed document?

- A. Message digest (MD)
- B. Asymmetric
- C. Symmetric
- D. Hashing

Answer: A

NEW QUESTION 316

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 318

- (Exam Topic 15)

Which of the following encryption technologies has the ability to function as a stream cipher?

- A. Cipher Feedback (CFB)
- B. Feistel cipher
- C. Cipher Block Chaining (CBC) with error propagation
- D. Electronic Code Book (ECB)

Answer: A

NEW QUESTION 320

- (Exam Topic 15)

Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

- A. Memory collection
- B. Forensic disk imaging
- C. Malware analysis
- D. Live response

Answer: A

NEW QUESTION 323

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 325

- (Exam Topic 15)

Which of the following is a limitation of the Bell-LaPadula model?

- A. Segregation of duties (SoD) is difficult to implement as the "no read-up" rule limits the ability of an object to access information with a higher classification.
- B. Mandatory access control (MAC) is enforced at all levels making discretionary access control (DAC) impossible to implement.
- C. It contains no provision or policy for changing data access control and works well only with access systems that are static in nature.
- D. It prioritizes integrity over confidentiality which can lead to inadvertent information disclosure.

Answer: A

NEW QUESTION 328

- (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 331

- (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 333

- (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 335

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 338

- (Exam Topic 15)

Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

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

Answer: A

NEW QUESTION 341

- (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 345

- (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 346

- (Exam Topic 15)

What is the BEST method to use for assessing the security impact of acquired software?

- A. Common vulnerability review
- B. Software security compliance validation
- C. Threat modeling
- D. Vendor assessment

Answer: B

NEW QUESTION 351

- (Exam Topic 15)

Which of the following BEST describes the standard used to exchange authorization information between different identity management systems?

- A. Security Assertion Markup Language (SAML)
- B. Service Oriented Architecture (SOA)
- C. Extensible Markup Language (XML)
- D. Wireless Authentication Protocol (WAP)

Answer: A

NEW QUESTION 354

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 359

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 362

- (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 367

- (Exam Topic 15)

Which of the following has the responsibility of information technology (IT) governance?

- A. Chief Information Officer (CIO)
- B. Senior IT Management
- C. Board of Directors
- D. Chief Information Security Officer (CISO)

Answer: A

NEW QUESTION 368

- (Exam Topic 15)

International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

- A. General Data Protection Regulation (GDPR)
- B. Palermo convention
- C. Wassenaar arrangement
- D. International Traffic in Arms Regulations (ITAR)

Answer: C

NEW QUESTION 369

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 373

- (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 374

- (Exam Topic 15)

How should the retention period for an organization's social media content be defined?

- A. By the retention policies of each social media service
- B. By the records retention policy of the organization
- C. By the Chief Information Officer (CIO)
- D. By the amount of available storage space

Answer: B

NEW QUESTION 376

- (Exam Topic 15)

If traveling abroad and a customs official demands to examine a personal computer, which of the following should be assumed?

- A. The hard drive has been stolen.
- B. The Internet Protocol (IP) address has been copied.
- C. The hard drive has been copied.
- D. The Media Access Control (MAC) address was stolen

Answer: C

NEW QUESTION 379

- (Exam Topic 15)

Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

- A. Map the organization's current security practices to industry standards and frameworks.
- B. Define the organization's objectives regarding security and risk mitigation.
- C. Select from a choice of security best practices.
- D. Review the past security assessments.

Answer: A

NEW QUESTION 382

- (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 384

- (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 385

- (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 386

- (Exam Topic 15)

Which of the following is the BEST method to gather evidence from a computer's hard drive?

- A. Disk duplication
- B. Disk replacement
- C. Forensic signature
- D. Forensic imaging

Answer: D

NEW QUESTION 388

- (Exam Topic 15)

An organization implements Network Access Control (NAC) by Institute of Electrical and Electronics Engineers (IEEE) 802.1x and discovers the printers do not support the IEEE 802.1x standard. Which of the following is the BEST resolution?

- A. Implement port security on the switch ports for the printers.
- B. Implement a virtual local area network (VLAN) for the printers.
- C. Do nothing; IEEE 802.1x is irrelevant to printers.
- D. Install an IEEE 802.1x bridge for the printers.

Answer: A

NEW QUESTION 389

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 390

- (Exam Topic 15)

What is the MAIN purpose of a security assessment plan?

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

Answer: B

NEW QUESTION 391

- (Exam Topic 15)

A security engineer is required to integrate security into a software project that is implemented by small groups test quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process?

- A. Service-oriented architecture (SOA)
- B. Spiral Methodology
- C. Structured Waterfall Programming Development
- D. Devops Integrated Product Team (IPT)

Answer: C

NEW QUESTION 395

- (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 399

- (Exam Topic 15)

What is the overall goal of software security testing?

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

Answer: B

NEW QUESTION 402

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 406

- (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 407

- (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 409

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 413

- (Exam Topic 15)

The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a particular system over a 12-month period. Which type of SOC report should be utilized?

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

Answer: C

NEW QUESTION 414

- (Exam Topic 15)

Which of the following is the MOST secure protocol for remote command access to the firewall?

- A. Secure Shell (SSH)
- B. Trivial File Transfer Protocol (TFTP)
- C. Hypertext Transfer Protocol Secure (HTTPS)
- D. Simple Network Management Protocol (SNMP) v1

Answer: A

NEW QUESTION 417

- (Exam Topic 15)

When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

- A. Resiliency of the system
- B. Detection of sophisticated attackers
- C. Risk assessment of the system
- D. Topology of the network used for the system

Answer: A

NEW QUESTION 420

- (Exam Topic 15)

A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

- A. Remove the ultraviolet light filters on the HVAC intake and replace the fire suppression system on the upper floors with a dry system
- B. Add additional ultraviolet light filters to the HVAC intake supply and return ducts and change server room fire suppression to FM-200
- C. Apply additional physical security around the HVAC intakes and update upper floor fire suppression to FM-200.
- D. Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system

Answer: C

NEW QUESTION 424

- (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 425

- (Exam Topic 15)

Which of the following VPN configurations should be used to separate Internet and corporate traffic?

- A. Split-tunnel
- B. Remote desktop gateway
- C. Site-to-site
- D. Out-of-band management

Answer: A

NEW QUESTION 429

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 433

- (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 438

- (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 439

- (Exam Topic 15)

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

What is the MOST common attack leverage against this flaw?

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

Answer: A

NEW QUESTION 441

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 442

- (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 444

- (Exam Topic 15)

An organization is considering partnering with a third-party supplier of cloud services. The organization will only be providing the data and the third-party supplier will be providing the security controls. Which of the following BEST describes this service offering?

- A. Platform as a Service (PaaS)
- B. Infrastructure as a Service (IaaS)
- C. Software as a Service (SaaS)
- D. Anything as a Service (XaaS)

Answer: D

NEW QUESTION 447

- (Exam Topic 15)

Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?

- A. System logs
- B. Anti-spyware
- C. Integrity checker
- D. Firewall logs

Answer: C

NEW QUESTION 449

- (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 450

- (Exam Topic 15)

In an environment where there is not full administrative control over all network connected endpoints, such as a university where non-corporate devices are used, what is the BEST way to restrict access to the network?

- A. Use switch port security to limit devices connected to a particular switch port.
- B. Use of virtual local area networks (VLAN) to segregate users.
- C. Use a client-based Network Access Control (NAC) solution.
- D. Use a clientless Network Access Control (NAC) solution

Answer: A

NEW QUESTION 455

- (Exam Topic 15)

When are security requirements the LEAST expensive to implement?

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

Answer: D

NEW QUESTION 458

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 461

- (Exam Topic 15)

What part of an organization's strategic risk assessment MOST likely includes information on items affecting the success of the organization?

- A. Key Risk Indicator (KRI)
- B. Threat analysis
- C. Vulnerability analysis
- D. Key Performance Indicator (KPI)

Answer: A

NEW QUESTION 464

- (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 469

- (Exam Topic 15)

An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

- A. Hybrid
- B. Federated
- C. Decentralized
- D. Centralized

Answer: A

NEW QUESTION 474

- (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 477

- (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 480

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 481

- (Exam Topic 15)

When MUST an organization's information security strategic plan be reviewed?

- A. Quarterly, when the organization's strategic plan is updated
- B. Whenever there are significant changes to a major application
- C. Every three years, when the organization's strategic plan is updated
- D. Whenever there are major changes to the business

Answer: D

NEW QUESTION 486

- (Exam Topic 15)

To comply with industry requirements, a security assessment on the cloud server should identify which protocols and weaknesses are being exposed to attackers on the Internet.

Which of the following tools is the MOST appropriate to complete the assessment?

- A. Use tcpdump and parse the output file in a protocol analyzer.
- B. Use an IP scanner and target the cloud WAN network addressing
- C. Run netstat in each cloud server and retrieve the running processes.
- D. Use nmap and set the servers' public IPs as the target

Answer: D

NEW QUESTION 488

- (Exam Topic 15)

A company developed a web application which is sold as a Software as a Service (SaaS) solution to the customer. The application is hosted by a web server running on a 'specific operating system (OS) on a virtual machine (VM). During the transition phase of the service, it is determined that the support team will need access to the application logs. Which of the following privileges would be the MOST suitable?

- A. Administrative privileges on the OS
- B. Administrative privileges on the web server
- C. Administrative privileges on the hypervisor
- D. Administrative privileges on the application folders

Answer: D

NEW QUESTION 491

- (Exam Topic 15)

What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

- A. Familiar syntax, abstraction of network topology, and definition of network protocols
- B. Network syntax, abstraction of network flow, and abstraction of network protocols
- C. Network syntax, abstraction of network commands, and abstraction of network protocols
- D. Familiar syntax, abstraction of network topology, and abstraction of network protocols

Answer: C

NEW QUESTION 494

- (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 498

- (Exam Topic 15)

A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should be an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

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

Answer: D

NEW QUESTION 500

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 501

- (Exam Topic 15)

Which of the following BEST describes botnets?

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

Answer: D

NEW QUESTION 504

- (Exam Topic 15)

Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

- A. Scheduled team review of coding style and techniques for vulnerability patterns
- B. Using automated programs to test for the latest known vulnerability patterns
- C. The regular use of production code routines from similar applications already in use
- D. Ensure code editing tools are updated against known vulnerability patterns

Answer: B

NEW QUESTION 509

- (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 510

- (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 511

- (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 515

- (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 516

- (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 521

- (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 522

- (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)

Continuity of operations is BEST supported by which of the following?

- A. Confidentiality, availability, and reliability
- B. Connectivity, reliability, and redundancy
- C. Connectivity, reliability, and recovery
- D. Confidentiality, integrity, and availability

Answer: B

NEW QUESTION 524

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 529

- (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 530

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 534

- (Exam Topic 14)

copyright provides protection for which of the following?

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

Answer: C

NEW QUESTION 535

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 538

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 539

- (Exam Topic 14)

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

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

Answer: D

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 542

- (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 543

- (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 545

- (Exam Topic 14)

Which of the following is the GREATEST security risk associated with the user of identity as a service (IDaaS) when an organization its own software?

- A. Incompatibility with Federated Identity Management (FIM)
- B. Increased likelihood of confidentiality breach
- C. Denial of access due to reduced availability
- D. Security Assertion Markup Language (SAM) integration

Answer: B

NEW QUESTION 547

- (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 549

- (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 551

- (Exam Topic 14)

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

- A. Access control
- B. Partial traffic flow confidentiality

- C. Protection against replay attack
- D. Data origin authentication

Answer: C

NEW QUESTION 556

- (Exam Topic 14)

Which of the following is mobile device remote fingerprinting?

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

Answer: C

NEW QUESTION 560

- (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 561

- (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 562

- (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 564

- (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 565

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 569

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 574

- (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 575

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 579

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 580

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 583

- (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 585

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 590

- (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 593

- (Exam Topic 14)

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

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

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

Answer: A

NEW QUESTION 598

- (Exam Topic 14)

Which of the following would an internal technical security audit BEST validate?

- A. Whether managerial controls are in place
- B. Support for security programs by executive management
- C. Appropriate third-party system hardening
- D. Implementation of changes to a system

Answer: D

NEW QUESTION 601

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 602

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 603

- (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 604

- (Exam Topic 14)

A new Chief Information Officer (CIO) created a group to write a data retention policy based on applicable laws. Which of the following is the PRIMARY motivation for the policy?

- A. To back up data that is used on a daily basis
- B. To dispose of data in order to limit liability
- C. To reduce costs by reducing the amount of retained data
- D. To classify data according to what it contains

Answer: B

NEW QUESTION 606

- (Exam Topic 14)

Which of the following models uses unique groups contained in unique conflict classes?

- A. Chinese Wall
- B. Bell-LaPadula
- C. Clark-Wilson
- D. Biba

Answer: C

NEW QUESTION 608

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 610

- (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 611

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 613

- (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 617

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 619

- (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 623

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 625

- (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 628

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 632

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 633

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 635

- (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 637

- (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 641

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 643

- (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 644

- (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 646

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 648

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 652

- (Exam Topic 14)

Which of the following trust services principles refers to the accessibility of information used by the systems, products, or services offered to a third-party provider's customers?

- A. Security
- B. Privacy
- C. Access

D. Availability

Answer: C

Explanation:

Reference: <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/tr>

NEW QUESTION 654

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 656

- (Exam Topic 14)

Which one of the following would cause an immediate review and possible change to the security policies of an organization?

- A. Change in technology
- B. Change in senior management
- C. Change to organization processes
- D. Change to organization goals

Answer: D

NEW QUESTION 659

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 663

- (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 668

- (Exam Topic 14)

An Intrusion Detection System (IDS) is based on the general hypothesis that a security violation is associated with a pattern of system usage which can be

- A. differentiated from a normal usage pattern.
- B. used to detect known violations.
- C. used to detect a masquerader.
- D. differentiated to detect all security violations.

Answer: A

NEW QUESTION 673

- (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 675

- (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 676

- (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 678

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 681

- (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 684

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 685

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 690

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 694

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 697

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 700

- (Exam Topic 14)

When conducting a forensic criminal investigation on a computer hard drive, what should be done PRIOR to analysis?

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

Answer: C

NEW QUESTION 703

- (Exam Topic 14)

Which area of embedded devices are most commonly attacked?

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

Answer: A

NEW QUESTION 707

- (Exam Topic 14)

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

- A. Consult the lead investigator to learn the details of the case and required evidence.
- B. Assure that grounding procedures have been followed to reduce the loss of digital data due to static electricity discharge.
- C. Update the Basic Input Output System (BIOS) and Operating System (OS) of any tools used to assure evidence admissibility.
- D. Confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims.

Answer: D

NEW QUESTION 711

- (Exam Topic 14)

A client has reviewed a vulnerability assessment report and has stated it is inaccurate. The client states that the vulnerabilities listed are not valid because the host's Operating System (OS) was not properly detected.

Where in the vulnerability assessment process did the error MOST likely occur?

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

Answer: A

NEW QUESTION 712

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 714

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 718

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 723

- (Exam Topic 14)

Which of the following processes has the PRIMARY purpose of identifying outdated software versions, missing patches, and lapsed system updates?

- A. Penetration testing
- B. Vulnerability management
- C. Software Development Life Cycle (SDLC)
- D. Life cycle management

Answer: B

Explanation:

Reference:

<https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/vulnerab>

NEW QUESTION 726

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 727

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 728

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 731

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 736

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 737

- (Exam Topic 13)

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

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

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 738

- (Exam Topic 13)

Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 740

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISSP Product From:

<https://www.2passeasy.com/dumps/CISSP/>

Money Back Guarantee

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