

ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)



NEW QUESTION 1

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 2

- (Exam Topic 15)

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)

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 4

- (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 5

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 6

- (Exam Topic 15)

In which process MUST security be considered during the acquisition of new software?

- A. Contract negotiation
- B. Request for proposal (RFP)
- C. Implementation
- D. Vendor selection

Answer: B

NEW QUESTION 7

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 8

- (Exam Topic 15)

Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

- A. Proper security controls, security goals, and fault mitigation are properly conducted.
- B. Proper security controls, security objectives, and security goals are properly initiated.
- C. Security goals, proper security controls, and validation are properly initiated.
- D. Security objectives, security goals, and system test are properly conducted.

Answer: B

NEW QUESTION 9

- (Exam Topic 15)

Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 15)

A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

- A. Service accounts removal
- B. Data validation
- C. Logging and monitoring
- D. Data sanitization

Answer: B

NEW QUESTION 10

- (Exam Topic 15)

A company is planning to implement a private cloud infrastructure. Which of the following recommendations will support the move to a cloud infrastructure?

- A. Implement a virtual local area network (VLAN) for each department and create a separate subnet for each VLAN.
- B. Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.
- C. Implement a virtual local area network (VLAN) to logically separate the local area network (LAN) from the physical switches.
- D. implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices and applications.

Answer: D

NEW QUESTION 12

- (Exam Topic 15)

What is a use for mandatory access control (MAC)?

- A. Allows for labeling of sensitive user accounts for access control
- B. Allows for mandatory user identity and passwords based on sensitivity
- C. Allows for mandatory system administrator access control over objects
- D. Allows for object security based on sensitivity represented by a label

Answer: D

NEW QUESTION 16

- (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 19

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 20

- (Exam Topic 15)

Which of the following is fundamentally required to address potential security issues when initiating software development?

- A. Implement ongoing security audits in all environments.
- B. Ensure isolation of development from production.
- C. Add information security objectives into development.
- D. Conduct independent source code review.

Answer: C

NEW QUESTION 24

- (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 26

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 30

- (Exam Topic 15)

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the

BEST design approach to securing this environment?

- A. Place firewalls around critical devices, isolating them from the rest of the environment.
- B. Layer multiple detective and preventative technologies at the environment perimeter.
- C. Use reverse proxies to create a secondary "shadow" environment for critical systems.
- D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

Answer: B

NEW QUESTION 35

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 38

- (Exam Topic 15)

Which of the following is the FIRST step for defining Service Level Requirements (SLR)?

- A. Creating a prototype to confirm or refine the customer requirements
- B. Drafting requirements for the service level agreement (SLA)
- C. Discussing technology and solution requirements with the customer
- D. Capturing and documenting the requirements of the customer

Answer: D

NEW QUESTION 42

- (Exam Topic 15)

During a penetration test, what are the three PRIMARY objectives of the planning phase?

- A. Determine testing goals, identify rules of engagement, and conduct an initial discovery scan.
- B. Finalize management approval, determine testing goals, and gather port and service information.
- C. Identify rules of engagement, finalize management approval, and determine testing goals.
- D. Identify rules of engagement, document management approval, and collect system and application information.

Answer: D

NEW QUESTION 47

- (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 52

- (Exam Topic 15)

Which of the following ensures old log data is not overwritten?

- A. Increase log file size
- B. Implement Syslog
- C. Log preservation
- D. Log retention

Answer: D

NEW QUESTION 56

- (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 58

- (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 60

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 62

- (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 65

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 67

- (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 71

- (Exam Topic 15)

During a Disaster Recovery (DR) simulation, it is discovered that the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans simultaneously. What would be impacted by this fact if left unchanged?

- A. Recovery Point Objective (RPO)
- B. Recovery Time Objective (RTO)
- C. Business Impact Analysis (BIA)
- D. Return on Investment (ROI)
- E. A

Answer: E

NEW QUESTION 75

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 78

- (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 81

- (Exam Topic 15)

What is the PRIMARY benefit of incident reporting and computer crime investigations?

- A. Providing evidence to law enforcement
- B. Repairing the damage and preventing future occurrences
- C. Appointing a computer emergency response team
- D. Complying with security policy

Answer: D

NEW QUESTION 82

- (Exam Topic 15)

Information security practitioners are in the midst of implementing a new firewall. Which of the following failure methods would BEST prioritize security in the event of failure?

- A. Fail-Closed
- B. Fail-Open
- C. Fail-Safe
- D. Failover

Answer: A

NEW QUESTION 85

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 87

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 88

- (Exam Topic 15)

Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

- A. Prevent unauthorized modification of data.
- B. Restore the system after an incident.
- C. Detect security events and incidents.
- D. Protect individual components from exploitation

Answer: D

NEW QUESTION 93

- (Exam Topic 15)

In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

- A. Prepare to take corrective actions quickly.
- B. Receive approval from the change review board.
- C. Review logs for any anomalies.
- D. Automate functionality testing.

Answer: B

NEW QUESTION 95

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 97

- (Exam Topic 15)

Which audit type is MOST appropriate for evaluating the effectiveness of a security program?

- A. Threat
- B. Assessment

- C. Analysis
- D. Validation

Answer: B

NEW QUESTION 101

- (Exam Topic 15)

A user is allowed to access the file labeled “Financial Forecast,” but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

- A. Minimum access control
- B. Rule-based access control
- C. Limited role-based access control (RBAC)
- D. Access control list (ACL)

Answer: B

NEW QUESTION 105

- (Exam Topic 15)

Which of the following types of firewall only examines the “handshaking” between packets before forwarding traffic?

- A. Proxy firewalls
- B. Host-based firewalls
- C. Circuit-level firewalls
- D. Network Address Translation (NAT) firewalls

Answer: C

NEW QUESTION 108

- (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 113

- (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 118

- (Exam Topic 15)

Which of the following BEST describes the objectives of the Business Impact Analysis (BIA)?

- A. Identifying the events and environmental factors that can adversely affect an organization
- B. Identifying what is important and critical based on disruptions that can affect the organization.
- C. Establishing the need for a Business Continuity Plan (BCP) based on threats that can affect an organization
- D. Preparing a program to create an organizational awareness for executing the Business Continuity Plan (BCP)

Answer: B

NEW QUESTION 120

- (Exam Topic 15)

A security practitioner needs to implement a solution to verify endpoint security protections and operating system (OS) versions. Which of the following is the BEST solution to implement?

- A. An intrusion prevention system (IPS)
- B. An intrusion prevention system (IPS)
- C. Network Access Control (NAC)
- D. A firewall

Answer: B

NEW QUESTION 123

- (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 128

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 129

- (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 130

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 135

- (Exam Topic 15)

Which of the following is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions?

- A. Information Security Management System (ISMS)
- B. Information Sharing & Analysis Centers (ISAC)
- C. Risk Management Framework (RMF)
- D. Information Security Continuous Monitoring (ISCM)

Answer: D

NEW QUESTION 136

- (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 138

- (Exam Topic 15)

- A. Require the cloud IAM provider to use declarative security instead of programmatic authentication checks.
- B. Integrate a Web-Application Firewall (WAF) In reverse-proxy mode in front of the service provider.
- C. Apply Transport layer Security (TLS) to the cloud-based authentication checks.
- D. Install an on-premise Authentication Gateway Service (AGS) In front of the service provider.

Answer: D

NEW QUESTION 139

- (Exam Topic 15)

Which of the following is security control volatility?

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

Answer: D

NEW QUESTION 140

- (Exam Topic 15)

An established information technology (IT) consulting firm is considering acquiring a successful local startup. To gain a comprehensive understanding of the startup's security posture' which type of assessment provides the BEST information?

- A. A security audit
- B. A penetration test
- C. A tabletop exercise
- D. A security threat model

Answer: A

NEW QUESTION 144

- (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 146

- (Exam Topic 15)

A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

- A. Virtual network computing
- B. Secure Socket Shell
- C. in-band connection
- D. Site-to-site VPN

Answer: D

NEW QUESTION 148

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 150

- (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 155

- (Exam Topic 15)

Spyware is BEST described as

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

Answer: B

NEW QUESTION 157

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 161

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 166

- (Exam Topic 15)

Which of the following are mandatory canons for the (ISC)* Code of Ethics?

- A. Develop comprehensive security strategies for the organization.
- B. Perform is, honestly, fairly, responsibly, and lawfully for the organization.
- C. Create secure data protection policies to principals.
- D. Provide diligent and competent service to principals.

Answer: D

NEW QUESTION 169

- (Exam Topic 15)

An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

- A. Data driven risk assessment with a focus on data
- B. Security controls driven assessment that focuses on controls management
- C. Business processes based risk assessment with a focus on business goals
- D. Asset driven risk assessment with a focus on the assets

Answer: A

NEW QUESTION 171

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 174

- (Exam Topic 15)

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

- A. Hybrid frequency band, service set identifier (SSID), and interpolation

- B. Performance, geographic location, and radio signal interference
- C. Facility size, intermodulation, and direct satellite service
- D. Existing client devices, manufacturer reputation, and electrical interference

Answer: D

NEW QUESTION 178

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 180

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 181

- (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 182

- (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 184

- (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 187

- (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 190

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 193

- (Exam Topic 15)

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

Answer: D

NEW QUESTION 197

- (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 201

- (Exam Topic 15)

The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

- A. Security information and event management (SIEM)
- B. Security perimeter
- C. Defense-in-depth
- D. Access control

Answer: B

NEW QUESTION 205

- (Exam Topic 15)

An information technology (IT) employee who travels frequently to various sites remotely to an organization's the following solutions BEST serves as a secure control mechanism to meet the organization's requirements? to troubleshoot p Which of the following solutions BEST serves as a secure control mechanism to meet the organization's requirements?

- A. Update the firewall rules to include the static Internet Protocol (IP) addresses of the locations where the employee connects from.
- B. Install a third-party screen sharing solution that provides remote connection from a public website.
- C. Implement a Dynamic Domain Name Services (DDNS) account to initiate a virtual private network (VPN) using the DDNS record.
- D. Install a bastion host in the demilitarized zone (DMZ) and allow multi-factor authentication (MFA) access.

Answer: D

NEW QUESTION 207

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 210

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 213

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 214

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 215

- (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 217

- (Exam Topic 15)

If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), which of the following becomes even MORE essential to the assurance of network?

- A. Classless Inter-Domain Routing (CIDR)
- B. Deterministic routing
- C. Internet Protocol (IP) routing lookups
- D. Boundary routing

Answer: C

NEW QUESTION 219

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 223

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 226

- (Exam Topic 15)

Using Address Space Layout Randomization (ASLR) reduces the potential for which of the following attacks?

- A. SQL injection (SQLi)
- B. Man-in-the-middle (MITM)

- C. Cross-Site Scripting (XSS)
- D. Heap overflow

Answer: D

NEW QUESTION 228

- (Exam Topic 15)

What is the benefit of an operating system (OS) feature that is designed to prevent an application from executing code from a non-executable memory region?

- A. Identifies which security patches still need to be installed on the system
- B. Stops memory resident viruses from propagating their payload
- C. Reduces the risk of polymorphic viruses from encrypting their payload
- D. Helps prevent certain exploits that store code in buffers

Answer: C

NEW QUESTION 229

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 234

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 239

- (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 244

- (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 245

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 249

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 254

- (Exam Topic 15)

The personal laptop of an organization executive is stolen from the office, complete with personnel and project records. Which of the following should be done FIRST to mitigate future occurrences?

- A. Encrypt disks on personal laptops.
- B. Issue cable locks for use on personal laptops.
- C. Create policies addressing critical information on personal laptops.
- D. Monitor personal laptops for critical information.

Answer: A

NEW QUESTION 259

- (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 262

- (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 263

- (Exam Topic 15)

What is static analysis intended to do when analyzing an executable file?

- A. Collect evidence of the executable file's usage, including dates of creation and last use.
- B. Search the documents and files associated with the executable file.
- C. Analyze the position of the file in the file system and the executable file's libraries.
- D. Disassemble the file to gather information about the executable file's function.

Answer: D

NEW QUESTION 266

- (Exam Topic 15)

Which of the following would be considered an incident if reported by a security information and event management (SIEM) system?

- A. An administrator is logging in on a server through a virtual private network (VPN).
- B. A log source has stopped sending data.
- C. A web resource has reported a 404 error.
- D. A firewall logs a connection between a client on the Internet and a web server using Transmission Control Protocol (TCP) on port 80.

Answer: C

NEW QUESTION 270

- (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 275

- (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 277

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 281

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 285

- (Exam Topic 15)

Which of the following outsourcing agreement provisions has the HIGHEST priority from a security operations perspective?

- A. Conditions to prevent the use of subcontractors
- B. Terms for contract renegotiation in case of disaster
- C. Escalation process for problem resolution during incidents
- D. Root cause analysis for application performance issue

Answer: D

NEW QUESTION 288

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 291

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 295

- (Exam Topic 15)

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

- A. Mowing users access to files based on their group membership

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

Answer: A

NEW QUESTION 296

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 297

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 300

- (Exam Topic 15)

Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

- A. Review applicable destination country laws, forensically clean devices prior to travel, and only download sensitive data over a virtual private network (VPN) upon arriving at the destination.
- B. Keep laptops, external storage devices, and smartphones in the hotel room when not in use.
- C. Leverage a Secure Socket Layer (SSL) connection over a virtual private network (VPN) to download sensitive data upon arriving at the destination.
- D. Use multi-factor authentication (MFA) to gain access to data stored on laptops or external storage devices and biometric fingerprint access control isms to unlock smartphones.

Answer: D

NEW QUESTION 303

- (Exam Topic 15)

An organization has implemented a protection strategy to secure the network from unauthorized external access. The new Chief Information Security Officer (CISO) wants to increase security by better protecting the network from unauthorized internal access. Which Network Access Control (NAC) capability BEST meets this objective?

- A. Application firewall
- B. Port security
- C. Strong passwords
- D. Two-factor authentication (2FA)

Answer: D

NEW QUESTION 305

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 307

- (Exam Topic 15)

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

- A. Data Quality Principle
- B. Openness Principle
- C. Purpose Specification Principle
- D. Collection Limitation Principle

Answer: D

NEW QUESTION 308

- (Exam Topic 15)

What are the essential elements of a Risk Assessment Report (RAR)?

- A. Table of contents, testing criteria, and index
- B. Table of contents, chapters, and executive summary
- C. Executive summary, graph of risks, and process
- D. Executive summary, body of the report, and appendices

Answer: D

NEW QUESTION 311

- (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 314

- (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 318

- (Exam Topic 15)

A network security engineer needs to ensure that a security solution analyzes traffic for protocol manipulation and various sorts of common attacks. In addition, all Uniform Resource Locator (URL) traffic must be inspected and users prevented from browsing inappropriate websites. Which of the following solutions should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis?

- A. Intrusion detection system (IDS)
- B. Circuit-Level Proxy
- C. Application-Level Proxy
- D. Host-based Firewall

Answer: B

NEW QUESTION 320

- (Exam Topic 15)

A company hired an external vendor to perform a penetration test of a new payroll system. The company's internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

- A. Failure to perform interface testing
- B. Failure to perform negative testing
- C. Inadequate performance testing
- D. Inadequate application level testing

Answer: A

NEW QUESTION 325

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 328

- (Exam Topic 15)

Which of the following events prompts a review of the disaster recovery plan (DRP)?

- A. New members added to the steering committee
- B. Completion of the security policy review
- C. Change in senior management

D. Organizational merger

Answer: D

NEW QUESTION 332

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 335

- (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 337

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 341

- (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 345

- (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 349

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 351

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 355

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 356

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 358

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 361

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 365

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 366

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 371

- (Exam Topic 15)

Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

- A. Key findings section
- B. Executive summary with full details
- C. Risk review section
- D. Findings definition section

Answer: A

NEW QUESTION 373

- (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 374

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 377

- (Exam Topic 15)

What is the MOST important factor in establishing an effective Information Security Awareness Program?

- A. Obtain management buy-in.
- B. Conduct an annual security awareness event.
- C. Mandate security training.
- D. Hang information security posters on the walls,

Answer: C

NEW QUESTION 380

- (Exam Topic 15)

Which of the following factors is á 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 384

- (Exam Topic 15)

Which of the following MUST be done before a digital forensics investigator may acquire digital evidence?

- A. Inventory the digital evidence.
- B. Isolate the digital evidence.
- C. Verify that the investigator has the appropriate legal authority to proceed.
- D. Perform hashing to verify the integrity of the digital evidence.

Answer: C

NEW QUESTION 385

- (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 387

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 389

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 393

- (Exam Topic 15)

What action should be taken by a business line that is unwilling to accept the residual risk in a system after implementing compensating controls?

- A. Notify the audit committee of the situation.
- B. Purchase insurance to cover the residual risk.
- C. Implement operational safeguards.
- D. Find another business line willing to accept the residual risk.

Answer: B

NEW QUESTION 398

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 401

- (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 405

- (Exam Topic 15)

Which is the PRIMARY mechanism for providing the workforce with the information needed to protect an agency's vital information resources?

- A. Incorporating security awareness and training as part of the overall information security program
- B. An information technology (IT) security policy to preserve the confidentiality, integrity, and availability of systems
- C. Implementation of access provisioning process for coordinating the creation of user accounts
- D. Execution of periodic security and privacy assessments to the organization

Answer: A

NEW QUESTION 408

- (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 413

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 416

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 417

- (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 419

- (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 424

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 429

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 430

- (Exam Topic 15)

Digital non-repudiation requires which of the following?

- A. A trusted third-party
- B. Appropriate corporate policies
- C. Symmetric encryption
- D. Multifunction access cards

Answer: A

NEW QUESTION 431

- (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 434

- (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 435

- (Exam Topic 15)

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

- A. Identify team members.
- B. Define the scope.
- C. Notify system administrators.
- D. Collect evidence.

Answer: B

NEW QUESTION 439

- (Exam Topic 15)

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

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

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

Answer: B

NEW QUESTION 443

- (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 445

- (Exam Topic 15)

Which technique helps system designers consider potential security concerns of their systems and applications?

- A. Penetration testing
- B. Threat modeling
- C. Manual inspections and reviews

D. Source code review

Answer: B

NEW QUESTION 449

- (Exam Topic 15)

The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

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

Answer: D

NEW QUESTION 453

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 458

- (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 459

- (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 464

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 467

- (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 471

- (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 476

- (Exam Topic 15)

A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

- A. Federation authorities
- B. Proxied federation
- C. Static registration
- D. Dynamic registration

Answer: D

NEW QUESTION 478

- (Exam Topic 15)

What are the first two components of logical access control?

- A. Confidentiality and authentication
- B. Authentication and identification
- C. Identification and confidentiality
- D. Authentication and availability

Answer: B

NEW QUESTION 479

- (Exam Topic 15)

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



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

Answer: D

NEW QUESTION 482

- (Exam Topic 15)

a large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.

What is this value called?

- A. False Rejection Rate (FRR)
- B. Accuracy acceptance threshold
- C. Equal error rate
- D. False Acceptance Rate (FAR)

Answer: C

NEW QUESTION 485

- (Exam Topic 15)

An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data protection methods.

Which of the following is the BEST data protection method?

- A. Encryption

- B. Backups
- C. Data obfuscation
- D. Strong authentication

Answer: C

NEW QUESTION 490

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 493

- (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 497

- (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 499

- (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 501

- (Exam Topic 15)

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

This is an example of which type of network topology?

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

Answer: A

NEW QUESTION 505

- (Exam Topic 15)

Why would a system be structured to isolate different classes of information from one another and segregate them by user jurisdiction?

- A. The organization can avoid e-discovery processes in the event of litigation.
- B. The organization's infrastructure is clearly arranged and scope of responsibility is simplified.
- C. The organization can vary its system policies to comply with conflicting national laws.
- D. The organization is required to provide different services to various third-party organizations.

Answer: C

NEW QUESTION 508

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 510

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 511

- (Exam Topic 15)

An employee's home address should be categorized according to which of the following references?

- A. The consent form terms and conditions signed by employees
- B. The organization's data classification model
- C. Existing employee data classifications
- D. An organization security plan for human resources

Answer: B

NEW QUESTION 515

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 520

- (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 524

- (Exam Topic 15)

A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory risk to the company. The manager MOST likely discovered this during which of the following?

- A. Security control assessment.
- B. Separation of duties analysis
- C. Network Access Control (NAC) review
- D. Federated identity management (FIM) evaluation

Answer: B

NEW QUESTION 529

- (Exam Topic 15)

Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

- A. Data processing
- B. Storage encryption
- C. File hashing
- D. Data retention policy

Answer: C

NEW QUESTION 533

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 538

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 541

- (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 542

- (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 545

- (Exam Topic 15)

Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

- A. Training
- B. Legal
- C. Business
- D. Storage

Answer: B

NEW QUESTION 549

- (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 552

- (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 555

- (Exam Topic 15)

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

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

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

Answer: C

NEW QUESTION 556

- (Exam Topic 15)

Which of the following is the FIRST step during digital identity provisioning?

- A. Authorizing the entity for resource access
- B. Synchronizing directories
- C. Issuing an initial random password
- D. Creating the entity record with the correct attributes

Answer: D

NEW QUESTION 560

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 562

- (Exam Topic 15)

Why are packet filtering routers used in low-risk environments?

- A. They are high-resolution source discrimination and identification tools.
- B. They are fast and flexible, and protect against Internet Protocol (IP) spoofing.
- C. They are fast, flexible, and transparent.
- D. They enforce strong user authentication and audit log generation.

Answer: B

NEW QUESTION 564

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 569

- (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 570

- (Exam Topic 15)

What is the PRIMARY objective of the post-incident phase of the incident response process in the security operations center (SOC)?

- A. improve the IR process.
- B. Communicate the IR details to the stakeholders.
- C. Validate the integrity of the IR.
- D. Finalize the IR.

Answer: A

NEW QUESTION 571

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 574

- (Exam Topic 15)

Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

- A. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools
- B. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools
- C. Maintaining the inventory through a combination of on-premise storage configuration, cloud management, and partner management tools
- D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

Answer: C

NEW QUESTION 578

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 579

- (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 582

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 587

- (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 591

- (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 595

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 599

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 601

- (Exam Topic 15)

Which of the following is the MOST secure protocol for zremote 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 605

- (Exam Topic 15)

What is the BEST design for securing physical perimeter protection?

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

Answer: B

NEW QUESTION 609

- (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 612

- (Exam Topic 15)

An organization wants to migrate to Session Initiation Protocol (SIP) to save on telephony expenses. Which of the following security related statements should be

considered in the decision-making process?

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

Answer: C

NEW QUESTION 616

- (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 617

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 621

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 624

- (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 629

- (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 631

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 634

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 635

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 639

- (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 644

- (Exam Topic 15)

In order to provide dual assurance in a digital signature system, the design MUST include which of the following?

- A. The public key must be unique for the signed document.
- B. signature process must generate adequate authentication credentials.
- C. The hash of the signed document must be present.
- D. The encrypted private key must be provided in the signing certificate.

Answer: B

NEW QUESTION 649

- (Exam Topic 15)

Which of the following is a covert channel type?

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

Answer: A

NEW QUESTION 653

- (Exam Topic 15)

In which of the following scenarios is locking server cabinets and limiting access to keys preferable to locking the server room to prevent unauthorized access?

- A. Server cabinets are located in an unshared workspace.
- B. Server cabinets are located in an isolated server farm.
- C. Server hardware is located in a remote area.
- D. Server cabinets share workspace with multiple projects.

Answer: D

NEW QUESTION 655

- (Exam Topic 15)

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

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

Answer:

B

NEW QUESTION 658

- (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 661

- (Exam Topic 15)

A hospital's building controls system monitors and operates the environmental equipment to maintain a safe and comfortable environment. Which of the following could be used to minimize the risk of utility supply interruption?

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

Answer: D

NEW QUESTION 663

- (Exam Topic 15)

Which is MOST important when negotiating an Internet service provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over Internet Protocol (VoIP) services?

- A. Mean time to repair (MTTR)
- B. Quality of Service (QoS) between applications
- C. Availability of network services
- D. Financial penalties in case of disruption

Answer: B

NEW QUESTION 667

- (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 668

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 673

- (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 674

- (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 678

- (Exam Topic 15)

Which of the following is a risk matrix?

- A. A database of risks associated with a specific information system.
- B. A table of risk management factors for management to consider.
- C. A two-dimensional picture of risk for organizations, products, projects, or other items of interest.
- D. A tool for determining risk management decisions for an activity or system.

Answer: C

NEW QUESTION 681

- (Exam Topic 15)

Which of the following should exist in order to perform a security audit?

- A. Industry framework to audit against
- B. External (third-party) auditor
- C. Internal certified auditor
- D. Neutrality of the auditor

Answer: D

NEW QUESTION 685

- (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 pokies 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 690

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 695

- (Exam Topic 15)

The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

- A. Data masking and encryption of personal data
- B. Only to use encryption protocols approved by EU
- C. Anonymization of personal data when transmitted to sources outside the EU
- D. Never to store personal data of EU citizens outside the EU

Answer: D

NEW QUESTION 699

- (Exam Topic 15)

When recovering from an outage, what is the Recovery Point Objective (RPO), in terms of data recovery?

- A. The RPO is the maximum amount of time for which loss of data is acceptable.
- B. The RPO is the minimum amount of data that needs to be recovered.
- C. The RPO is a goal to recover a targeted percentage of data lost.
- D. The RPO is the amount of time it takes to recover an acceptable percentage of data lost.

Answer: B

NEW QUESTION 704

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 709

- (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 713

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 717

- (Exam Topic 15)

Which of the following is the MOST effective strategy to prevent an attacker from disabling a network?

- A. Test business continuity and disaster recovery (DR) plans.
- B. Design networks with the ability to adapt, reconfigure, and fail over.
- C. Implement network segmentation to achieve robustness.
- D. Follow security guidelines to prevent unauthorized network access.

Answer: D

NEW QUESTION 720

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 723

- (Exam Topic 15)

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

- A. Wireless Access Points (AP)
- B. Token-based authentication
- C. Host-based firewalls
- D. Trusted platforms

Answer: C

NEW QUESTION 725

- (Exam Topic 15)

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

- A. Mobile Device Management (MDM) with device wipe

- B. Whole device encryption with key escrow
- C. Virtual private network (VPN) with traffic encryption
- D. Mobile device tracking with geolocation

Answer: A

NEW QUESTION 727

- (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 731

- (Exam Topic 15)

What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

- A. Randomizing data
- B. Swapping data
- C. Encrypting data
- D. Encoding data

Answer: C

NEW QUESTION 735

- (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 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 737

- (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 742

- (Exam Topic 15)

Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

- A. Statement on Auditing Standards (SAS) 70
- B. Service Organization Control (SOC) 2
- C. Service Organization Control (SOC) 1
- D. Statement on Standards for Attestation Engagements (SSAE) 18

Answer: B

NEW QUESTION 743

- (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 747

- (Exam Topic 15)

Which of the following is the MAIN benefit of off-site storage?

- A. Cost effectiveness
- B. Backup simplicity
- C. Fast recovery
- D. Data availability

Answer: A

NEW QUESTION 749

- (Exam Topic 15)

A large organization's human resources and security teams are planning on implementing technology to eliminate manual user access reviews and improve compliance. Which of the following options is MOST likely to resolve the issues associated with user access?

- A. Implement a role-based access control (RBAC) system.
- B. Implement identity and access management (IAM) platform.
- C. Implement a Privileged Access Management (PAM) system.
- D. Implement a single sign-on (SSO) platform.

Answer: B

NEW QUESTION 753

- (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 755

- (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 758

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 763

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 767

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 770

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 775

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 776

- (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 780

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 781

- (Exam Topic 14)

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

- A. Maintenance hooks
- B. Polyinstiation
- C. Known vulnerability list
- D. Security auditing

Answer: B

NEW QUESTION 783

- (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 787

- (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 790

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 795

- (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 797

- (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 798

- (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 803

- (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 804

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 807

- (Exam Topic 14)

How long should the records on a project be retained?

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

Answer: B

NEW QUESTION 809

- (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 810

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 811

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 814

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 818

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 819

- (Exam Topic 14)

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

- A. Resumption procedures describing the actions to be taken to return to normal business operations
- B. Emergency procedures describing the necessary actions to be taken following an incident jeopardizes business operations
- C. Fallback procedures describing what action are to be taken to more essential business activities to alternative temporary locations

D. Maintain schedule how and the plan will be tested and the process for maintaining the plan

Answer: B

NEW QUESTION 820

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CISSP Practice Exam Features:

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

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