# ISC2

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

# About Exambible

*Your Partner of IT Exam*

# Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

# Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

**Answer:** D

**NEW QUESTION 8**
- (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 9**
- (Exam Topic 15)
Which of the following virtual network configuration options is BEST to protect virtual machines (VM)?

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

**Answer:** D

**NEW QUESTION 10**
- (Exam Topic 15)
While reviewing the financial reporting risks of a third-party application, which of the following Service Organization Control (SOC) reports will be the MOST useful?

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

**Answer:** A

**NEW QUESTION 10**
- (Exam Topic 15)
Which of the following access control models is MOST restrictive?

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

**Answer:** B

**NEW QUESTION 15**
- (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 18**
- (Exam Topic 15)
A large human resources organization wants to integrate their identity management with a trusted partner organization. The human resources organization wants to maintain the creation and management of the identities and may want to share with other partners in the future. Which of the following options BEST serves their needs?

A. Federated identity
B. Cloud Active Directory (AD)
C. Security Assertion Markup Language (SAML)
D. Single sign-on (SSO)

**Answer:** A

**NEW QUESTION 22**
- (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 27**
- (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)
Which of the following provides the MOST secure method for Network Access Control (NAC)?

A. Media Access Control (MAC) filtering
B. 802.IX authentication
C. Application layer filtering
D. Network Address Translation (NAT)

**Answer:** B


**NEW QUESTION 31**
- (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 33**
- (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 36**
- (Exam Topic 15)
When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

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

**Answer:** C


**NEW QUESTION 37**
- (Exam Topic 15)
Which of the following is the BEST way to protect an organization's data assets?

A. Monitor and enforce adherence to security policies.
B. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.
C. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.
D. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

**Answer:** B


**NEW QUESTION 41**

- (Exam Topic 15)
Which of the following is the strongest physical access control?

A. Biometrics and badge reader
B. Biometrics, a password, and personal identification number (PIN)
C. Individual password for each user
D. Biometrics, a password, and badge reader

**Answer:** D


**NEW QUESTION 44**
- (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 46**
- (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 47**
- (Exam Topic 15)
What type of database attack would allow a customer service employee to determine quarterly sales results
before they are publically announced?

A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining

**Answer:** A


**NEW QUESTION 52**
- (Exam Topic 15)
What is the MAIN purpose of conducting a business impact analysis (BIA)?

A. To determine the critical resources required to recover from an incident within a specified time period
B. To determine the effect of mission-critical information system failures on core business processes
C. To determine the cost for restoration of damaged information system
D. To determine the controls required to return to business critical operations

**Answer:** B


**NEW QUESTION 55**
- (Exam Topic 15)
Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

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

**Answer:** A


**NEW QUESTION 59**
- (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 61**
- (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 63**
- (Exam Topic 15)
Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

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

**Answer:** D

**NEW QUESTION 67**
- (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 70**
- (Exam Topic 15)
Recently, an unknown event has disrupted a single Layer-2 network that spans between two geographically diverse data centers. The network engineers have asked for assistance in identifying the root cause of the event. Which of the following is the MOST likely cause?

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

**Answer:** D

**NEW QUESTION 75**
- (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 76**
- (Exam Topic 15)
What is the P R IM A R Y reason criminal law is difficult to enforce when dealing with cyber-crime?

A. Extradition treaties are rarely enforced.
B. Numerous language barriers exist.
C. Law enforcement agencies are understaffed.
D. Jurisdiction is hard to define.

**Answer:** D

**NEW QUESTION 79**
- (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 80**
- (Exam Topic 15)
What would be the BEST action to take in a situation where collected evidence was left unattended overnight in an unlocked vehicle?

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

**Answer:** D


**NEW QUESTION 82**
- (Exam Topic 15)
Which of the following is the BEST way to protect against Structured Query language (SQL) injection?

A. Enforce boundary checking.
B. Ratfrict um of SELECT command.
C. Restrict HyperText Markup Language (HTML) source code
D. Use stored procedures.

**Answer:** D


**NEW QUESTION 85**
- (Exam Topic 15)
A software developer installs a game on their organization-provided smartphone. Upon installing the game, the software developer is prompted to allow the game access to call logs, Short Message Service (SMS) messaging, and Global Positioning System (GPS) location data. What has the game MOST likely introduced to the smartphone?

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

**Answer:** B


**NEW QUESTION 89**
- (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 90**
- (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 91**
- (Exam Topic 15)
Why is data classification control important to an organization?

A. To ensure its integrity, confidentiality and availability
B. To enable data discovery
C. To control data retention in alignment with organizational policies and regulation
D. To ensure security controls align with organizational risk appetite

**Answer:** A


**NEW QUESTION 92**

- (Exam Topic 15)
Why is authentication by ownership stronger than authentication by knowledge?

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

**Answer:** B

**NEW QUESTION 96**
- (Exam Topic 15)
What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

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

**Answer:** A

**NEW QUESTION 99**
- (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 104**
- (Exam Topic 15)
A digitally-signed e-mail was delivered over a wireless network protected with Wired Equivalent Privacy (WEP) protocol. Which of the following principles is at risk?

A. Availability
B. Non-Repudiation
C. Confidentiality
D. Integrity

**Answer:** B

**NEW QUESTION 109**
- (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 113**
- (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 114**
- (Exam Topic 15)
Which of the following is an indicator that a company's new user security awareness training module has been effective?

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

**Answer:** B

**NEW QUESTION 118**
- (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 121**
- (Exam Topic 15)
As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem?

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

**Answer:** C

**NEW QUESTION 125**
- (Exam Topic 15)
The disaster recovery (DR) process should always include

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

**Answer:** A

**NEW QUESTION 130**
- (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 134**
- (Exam Topic 15)
Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

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

**Answer:** A

**NEW QUESTION 138**
- (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 140**
- (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 143**
- (Exam Topic 15)
What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

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

**Answer:** D


**NEW QUESTION 144**
- (Exam Topic 15)
What is the correct order of execution for security architecture?

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

**Answer:** A


**NEW QUESTION 146**
- (Exam Topic 15)
What is the term used to define where data is geographically stored in the cloud?

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

**Answer:** D


**NEW QUESTION 148**
- (Exam Topic 15)
A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

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

**Answer:** A


**NEW QUESTION 151**
- (Exam Topic 15)
Which of the following is included in change management?

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

**Answer:** A


**NEW QUESTION 152**
- (Exam Topic 15)
In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below.
Which of the following would be a reasonable annual loss expectation?

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

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

**Answer:** B


**NEW QUESTION 153**
- (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 157**
- (Exam Topic 15)
What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

A. Capturing an image of the system
B. Maintaining the chain of custody
C. Complying with the organization's security policy
D. Outlining all actions taken during the investigation

**Answer:** A


**NEW QUESTION 159**
- (Exam Topic 15)
In which of the following system life cycle processes should security requirements be developed?

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

**Answer:** B


**NEW QUESTION 160**
- (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 164**
- (Exam Topic 15)
Which of the following is the MOST effective countermeasure against data remanence?

A. Destruction
B. Clearing
C. Purging
D. Encryption

**Answer:** A


**NEW QUESTION 169**
- (Exam Topic 15)
What is the BEST way to restrict access to a file system on computing systems?

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

**Answer:** C


**NEW QUESTION 170**

- (Exam Topic 15)
Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management
decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

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

**Answer:** A


**NEW QUESTION 171**
- (Exam Topic 15)
A software development company has a short timeline in which to deliver a software product. The software development team decides to use open-source software libraries to reduce the development time. What concept should software developers consider when using open-source software libraries?

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

**Answer:** A


**NEW QUESTION 176**
- (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 181**
- (Exam Topic 15)
Which of the following are the B EST characteristics of security metrics?

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

**Answer:** D


**NEW QUESTION 184**
- (Exam Topic 15)
Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

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

**Answer:** B


**NEW QUESTION 185**
- (Exam Topic 15)
What security principle addresses the issue of "Security by Obscurity"?

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

**Answer:** D


**NEW QUESTION 187**
- (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 188**
- (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 189**
- (Exam Topic 15)
Computer forensics requires which of the following MAIN steps?

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

**Answer:** B

**NEW QUESTION 192**
- (Exam Topic 15)
Which of the following is the MOST appropriate control for asset data labeling procedures?

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

**Answer:** C

**NEW QUESTION 195**
- (Exam Topic 15)
An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

A. RAID level 1
B. RAID level 3
C. RAID level 4
D. RAID level 5

**Answer:** D

**NEW QUESTION 198**
- (Exam Topic 15)
An information technology (IT) employee who travels frequently to various ies remotely to an organization' 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 mechanisn 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 199**
- (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 204**

- (Exam Topic 15)
In software development, which of the following entities normally signs the code to protect the code integrity?

A. The organization developing the code
B. The quality control group
C. The data owner
D. The developer

**Answer:** B


**NEW QUESTION 205**
- (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 208**
- (Exam Topic 15)
A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

A. Email the policy to the colleague as they were already part of the organization and familiar with it.
B. Do not acknowledge receiving the request from the former colleague and ignore them.
C. Access the policy on a company-issued device and let the former colleague view the screen.
D. Submit the request using company official channels to ensure the policy is okay to distribute.

**Answer:** B


**NEW QUESTION 213**
- (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 214**
- (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 216**
- (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 217**
- (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 221**
- (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 223**
- (Exam Topic 15)
An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

A. IM clients can interoperate between multiple vendors.
B. IM clients can run without administrator privileges.
C. IM clients can utilize random port numbers.
D. IM clients can run as executable that do not require installation.

**Answer:** B


**NEW QUESTION 225**
- (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 229**
- (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 230**
- (Exam Topic 15)
An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

A. It should be expressed as general requirements.
B. It should be expressed in legal terminology.
C. It should be expressed in business terminology.
D. It should be expressed as technical requirements.

**Answer:** D


**NEW QUESTION 233**
- (Exam Topic 15)
What BEST describes the confidentiality, integrity, availability triad?

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

**Answer:** C


**NEW QUESTION 234**
- (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 236**
- (Exam Topic 15)
Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management's directive?

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

**Answer:** B

**NEW QUESTION 237**
- (Exam Topic 15)
Which of the following is the reason that transposition ciphers are easily recognizable?

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

**Answer:** B

**NEW QUESTION 242**
- (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 246**
- (Exam Topic 15)
A hospital has allowed virtual private networking (VPN) access to remote database developers. Upon auditing the internal firewall configuration, the network administrator discovered that split-tunneling was enabled. What is the concern with this configuration?

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

**Answer:** C

**NEW QUESTION 249**
- (Exam Topic 15)
What is the benefit of using Network Admission Control (NAC)?

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

**Answer:** C

**NEW QUESTION 253**
- (Exam Topic 15)
Which of the following is the PRIMARY issue when analyzing detailed log information?

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

**Answer:** D

**NEW QUESTION 256**

- (Exam Topic 15)
Which of the following addresses requirements of security assessments during software acquisition?

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

**Answer:** A

**NEW QUESTION 261**
- (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 266**
- (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 269**
- (Exam Topic 15)
Which of the following will an organization's network vulnerability testing process BEST enhance?

A. Firewall log review processes
B. Asset management procedures
C. Server hardening processes
D. Code review procedures

**Answer:** C

**NEW QUESTION 273**
- (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 278**
- (Exam Topic 15)
Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this TAM action?

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

**Answer:** A

**NEW QUESTION 283**
- (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 287**
- (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 291**
- (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 295**
- (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 297**
- (Exam Topic 15)
At the destination host, which of the following OSI model layers will discard a segment with a bad checksum
in the UDP header?

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

**Answer:** C


**NEW QUESTION 300**
- (Exam Topic 15)
An organization is planning to have an it audit of its as a Service (SaaS) application to demonstrate to external parties that the security controls around availability are designed. The audit report must also cover a certain period of time to show the operational effectiveness of the controls. Which Service Organization Control (SOC) report would BEST fit their needs?

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

**Answer:** D


**NEW QUESTION 304**
- (Exam Topic 15)
A Distributed Denial of Service (DDoS) attack was carried out using malware called Mirai to create a large-scale command and control system to launch a botnet. Which of the following devices were the PRIMARY sources used to generate the attack traffic?

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

D. Mobile devices running Android

**Answer:** A


**NEW QUESTION 307**
- (Exam Topic 15)
An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

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

**Answer:** B


**NEW QUESTION 309**
- (Exam Topic 15)
Which of the following is the BEST approach to implement multiple servers on a virtual system?

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

**Answer:** C


**NEW QUESTION 314**
- (Exam Topic 15)
Which of the following is required to verify the authenticity of a digitally signed document?

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

**Answer:** A


**NEW QUESTION 318**
- (Exam Topic 15)
An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is MOST critical in creating acceptance tests or acceptance criteria for each release?

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

**Answer:** D


**NEW QUESTION 321**
- (Exam Topic 15)
A company hired an external vendor to perform a penetration test ofa 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 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 328**

- (Exam Topic 15)
The ability to send malicious code, generally in the form of a client side script, to a different end user is categorized as which type of vulnerability?

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

**Answer:** C

## NEW QUESTION 330
- (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 331
- (Exam Topic 15)
Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

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

**Answer:** C

## NEW QUESTION 332
- (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 334
- (Exam Topic 15)
The Chief Information Security Officer (CISO) is concerned about business application availability. The organization was recently subject to a ransomware attack that resulted in the unavailability of applications and services for 10 working days that required paper-based running of all main business processes. There are now aggressive plans to enhance the Recovery Time Objective (RTO) and cater for more frequent data captures. Which of the following solutions should be implemented to fully comply to the new business requirements?

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

**Answer:** A

## NEW QUESTION 335
- (Exam Topic 15)
A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

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

**Answer:** C

## NEW QUESTION 339
- (Exam Topic 15)
An organization's internal audit team performed a security audit on the company's system and reported that the manufacturing application is rarely updated along with other issues categorized as minor. Six months later, an external audit team reviewed the same system with the same scope, but identified severe weaknesses in the manufacturing application's security controls. What is MOST likely to be the root cause of the internal audit team's failure in detecting these security issues?

A. Inadequate test coverage analysis

B. Inadequate security patch testing
C. Inadequate log reviews
D. Inadequate change control procedures

**Answer:** A

**NEW QUESTION 341**
- (Exam Topic 15)
According to the (ISC)? ethics canon "act honorably, honestly, justly, responsibly, and legally," which order should be used when resolving conflicts?

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

**Answer:** A

**NEW QUESTION 346**
- (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 350**
- (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 355**
- (Exam Topic 15)
The Open Web Application Security Project's (OWASP) Software Assurance Maturity Model (SAMM) allows organizations to implement a flexible software security strategy to measure organizational impact based on what risk management aspect?

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

**Answer:** D

**NEW QUESTION 359**
- (Exam Topic 15)
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

A. OTDR
B. Tone generator
C. Fusion splicer
D. Cable tester
E. PoE injector

**Answer:** A

**NEW QUESTION 360**
- (Exam Topic 15)
Which of the following BEST describes the purpose of software forensics?

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

**Answer:** D

**NEW QUESTION 365**

- (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 367**
- (Exam Topic 15)
Which of the following types of datacenter architectures will MOST likely be used in a large SDN and can be extended beyond the datacenter?

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

**Answer:** B


**NEW QUESTION 371**
- (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 376**
- (Exam Topic 15)
A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

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

**Answer:** D


**NEW QUESTION 381**
- (Exam Topic 15)
Which of the following is the MOST common use of the Online Certificate Status Protocol (OCSP)?

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

**Answer:** D


**NEW QUESTION 382**
- (Exam Topic 15)
An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.
Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

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

**Answer:** B


**NEW QUESTION 385**
- (Exam Topic 15)
What is the MOST significant benefit of role-based access control (RBAC)?

A. Reduction in authorization administration overhead
B. Reduces inappropriate access
C. Management of least privilege
D. Most granular form of access control

**Answer:** A

**NEW QUESTION 389**
- (Exam Topic 15)
Upon commencement of an audit within an organization, which of the following actions is MOST important for the auditor(s) to take?

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

**Answer:** C

**NEW QUESTION 390**
- (Exam Topic 15)
When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

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

**Answer:** C

**NEW QUESTION 391**
- (Exam Topic 15)
Which of the following BEST obtains an objective audit of security controls?

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

**Answer:** A

**NEW QUESTION 395**
- (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-irHht-Middk (MITM)
C. War driving
D. Internet Protocol (IP) spoofing

**Answer:** B

**NEW QUESTION 396**
- (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 400**
- (Exam Topic 15)
Which of the following is a unique feature of attribute-based access control (ABAC)?

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

**Answer:** C

**NEW QUESTION 405**
- (Exam Topic 15)
Which of the (ISC)? Code of Ethics canons is MOST reflected when preserving the value of systems, applications, and entrusted information while avoiding conflicts of interest?

A. Act honorably, honestly, justly, responsibly, and legally.
B. Protect society, the commonwealth, and the infrastructure.
C. Provide diligent and competent service to principles.
D. Advance and protect the profession.

**Answer:** B


**NEW QUESTION 410**
- (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 411**
- (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 415**
- (Exam Topic 15)
What is the FIRST step in risk management?

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

**Answer:** C


**NEW QUESTION 417**
- (Exam Topic 15)
An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

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

**Answer:** C


**NEW QUESTION 421**
- (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 424**
- (Exam Topic 15)
Which of the following is the MOST appropriate technique for destroying magnetic platter style hard disk drives (HDD) containing data with a "HIGH" security categorization?

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

**Answer:** D


**NEW QUESTION 429**

- (Exam Topic 15)
Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

A. Store sensitive data only when necessary.
B. Educate end-users on methods of attacks on sensitive data.
C. Establish report parameters for sensitive data.
D. Monitor mail servers for sensitive data being exfilltrated.

**Answer:** A


**NEW QUESTION 434**
- (Exam Topic 15)
An organization wants to share data securely with their partners via the Internet. Which standard port is typically used to meet this requirement?

A. Setup a server on User Datagram Protocol (UDP) port 69
B. Setup a server on Transmission Control Protocol (TCP) port 21
C. Setup a server on Transmission Control Protocol (TCP) port 22
D. Setup a server on Transmission Control Protocol (TCP) port 80

**Answer:** C


**NEW QUESTION 436**
- (Exam Topic 15)
The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the focresight to enable what feature on all endpoints?

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

**Answer:** C


**NEW QUESTION 440**
- (Exam Topic 15)
During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

A. Planning
B. Operation
C. Assessment
D. Improvement

**Answer:** B


**NEW QUESTION 441**
- (Exam Topic 15)
Which of the following are the three MAIN categories of security controls?

A. Administrative, technical, physical
B. Corrective, detective, recovery
C. Confidentiality, integrity, availability
D. Preventative, corrective, detective

**Answer:** A


**NEW QUESTION 446**
- (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 451**
- (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 455**
- (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 457**
- (Exam Topic 15)
What does the result of Cost-Benefit Analysis (C8A) on new security initiatives provide?

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

**Answer:** A


**NEW QUESTION 461**
- (Exam Topic 15)
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

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

**Answer:** C


**NEW QUESTION 462**
- (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 464**
- (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 469**
- (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 473**

- (Exam Topic 15)
When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

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

**Answer:** B

**NEW QUESTION 474**
- (Exam Topic 15)
Which of the following is the MOST effective measure for dealing with rootkit attacks?

A. Turing off unauthorized services and rebooting the system
B. Finding and replacing the altered binaries with legitimate ones
C. Restoring the system from the last backup
D. Reinstalling the system from trusted sources

**Answer:** D

**NEW QUESTION 475**
- (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 478**
- (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 480**
- (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 483**
- (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 487**
- (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 491**
- (Exam Topic 15)
Which of the following statements BEST describes least privilege principle in a cloud environment?

A. Network segments remain private if unneeded to access the internet.
B. Internet traffic is inspected for all incoming and outgoing packets.
C. A single cloud administrator is configured to access core functions.
D. Routing configurations are regularly updated with the latest routes.

**Answer:** B


**NEW QUESTION 494**
- (Exam Topic 15)
Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

A. Control traffic
B. Prevent rapid movement
C. Prevent plggybacking
D. Control air flow

**Answer:** C


**NEW QUESTION 498**
- (Exam Topic 15)
Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

A. Take photos of the damage
B. Notify all of the Board of Directors
C. Communicate with the press following the communications plan
D. Dispatch personnel to the disaster recovery (DR) site

**Answer:** A


**NEW QUESTION 499**
- (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 501**
- (Exam Topic 15)
An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

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

**Answer:** A


**NEW QUESTION 502**
- (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 506**
- (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 507**
- (Exam Topic 15)
Which of the following BEST ensures the integrity of transactions to intended recipients?

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

**Answer:** A


**NEW QUESTION 512**
- (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 515**
- (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 520**
- (Exam Topic 15)
An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 1
B. 2
C. 3

**Answer:** A


**NEW QUESTION 521**
- (Exam Topic 15)
Which software defined networking (SDN) architectural component is responsible for translating network requirements?

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

**Answer:** D


**NEW QUESTION 524**
- (Exam Topic 15)
What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

A. Make all stakeholders aware of the program's progress.
B. Measure the effect of the program on the organization's workforce.
C. Facilitate supervision of periodic training events.
D. Comply with legal regulations and document due diligence in security practices.

**Answer:** C


**NEW QUESTION 527**
- (Exam Topic 15)
Which of the following protocols will allow the encrypted transfer of content on the Internet?

A. Server Message Block (SMB)

B. Secure copy
C. Hypertext Transfer Protocol (HTTP)
D. Remote copy

**Answer:** B

**NEW QUESTION 532**
- (Exam Topic 15)
Which of the following is considered the PRIMARY security issue associated with encrypted e-mail messages?

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

**Answer:** C

**NEW QUESTION 537**
- (Exam Topic 15)
What is the second phase of public key infrastructure (PKI) key/certificate life-cycle management?

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

**Answer:** A

**NEW QUESTION 539**
- (Exam Topic 15)
International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

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

**Answer:** C

**NEW QUESTION 541**
- (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 546**
- (Exam Topic 15)
A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

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

**Answer:** B

**NEW QUESTION 551**
- (Exam Topic 15)
A hacker can use a lockout capability to start which of the following attacks?

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

**Answer:** A

**NEW QUESTION 555**

- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

**Answer:** B


**NEW QUESTION 559**
- (Exam Topic 15)
In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

A. Development/Acquisition
B. Initiation
C. Implementation/ Assessment
D. Disposal

**Answer:** A


**NEW QUESTION 562**
- (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 564**
- (Exam Topic 15)
An Internet media company produces and broadcasts highly popular television shows. The company is suffering a huge revenue loss due to piracy. What technique should be used to track the distribution of content?

A. Install the latest data loss prevention (DLP) software at every server used to distribute content.
B. Log user access to server
C. Every day those log records are going to be audited by a team of specialized investigators.
D. Hire several investigators to identify sources of pirated content and report people sharing the content.
E. Use watermarking to hide a signature into the digital media such that it can be used to find who is using the company's content.

**Answer:** D


**NEW QUESTION 568**
- (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 573**
- (Exam Topic 15)
When conducting a remote access session using Internet Protocol Security (IPSec), which Open Systems Interconnection (OSI) model layer does this connection use?

A. Transport
B. Network
C. Data link
D. Presentation

**Answer:** B


**NEW QUESTION 578**
- (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 581**
- (Exam Topic 15)
The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

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

**Answer:** D

**NEW QUESTION 584**
- (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 587**
- (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 592**
- (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 595**
- (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 tog generation.

**Answer:** B

**NEW QUESTION 597**
- (Exam Topic 15)
An organization implements Network Access Control (NAC) ay Institute of Electrical and Electronics Engineers (IEEE) 802.1x and discovers the printers do not support the IEEE 802.1x standard. Which of the following is the BEST resolution?

A. Implement port security on the switch ports for the printers.
B. Implement a virtual local area network (VLAN) for the printers.
C. Do nothing; IEEE 802.1x is irrelevant to printers.
D. Install an IEEE 802. 1x bridge for the printers.

**Answer:** A

**NEW QUESTION 602**

- (Exam Topic 15)
The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery. Which of the following is the
MOST challenging aspect of this investigation?

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

**Answer:** C


**NEW QUESTION 607**
- (Exam Topic 15)
Which of the following security tools will ensure authorized data is sent to the application when implementing a cloud based application?

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

**Answer:** B


**NEW QUESTION 612**
- (Exam Topic 15)
All hosts on the network are sending logs via syslog-ng to the log collector. The log collector is behind its own firewall, The security professional wants to make sure not to put extra load on the firewall due to the amount of traffic that is passing through it. Which of the following types of filtering would MOST likely be used?

A. Uniform Resource Locator (URL) Filtering
B. Web Traffic Filtering
C. Dynamic Packet Filtering
D. Static Packet Filtering

**Answer:** C


**NEW QUESTION 613**
- (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 617**
- (Exam Topic 15)
An organization with divisions in the United States (US) and the United Kingdom (UK) processes data comprised of personal information belonging to subjects living in the European Union (EU) and in the US. Which data MUST be handled according to the privacy protections of General Data Protection Regulation (GDPR)?

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

**Answer:** A


**NEW QUESTION 620**
- (Exam Topic 15)
What is the overall goal of software security testing?

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

**Answer:** B


**NEW QUESTION 623**
- (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 627
- (Exam Topic 15)
A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

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

**Answer:** D

## NEW QUESTION 629
- (Exam Topic 15)
What industry-recognized document could be used as a baseline reference that is related to data security and business operations for conducting a security assessment?

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

**Answer:** D

## NEW QUESTION 634
- (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 635
- (Exam Topic 15)
In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

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

**Answer:** D

## NEW QUESTION 639
- (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. Gram 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 rs hired.
D. Prevent changes to the confidential data until a replacement application owner is hired.

**Answer:** B

## NEW QUESTION 642
- (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 644**
- (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 646**
- (Exam Topic 15)
employee training, risk management, and data handling procedures and policies could be characterized as which type of security measure?

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

**Answer:** D

**NEW QUESTION 648**
- (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 651**
- (Exam Topic 15)
What is a security concern when considering implementing software-defined networking (SDN)?

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

**Answer:** C

**NEW QUESTION 653**
- (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 656**
- (Exam Topic 15)
Which of the following VPN configurations should be used to separate Internet and corporate traffic?

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

**Answer:** A

**NEW QUESTION 661**
- (Exam Topic 15)
A security professional is assessing the risk in an application and does not take into account any mitigating or compensating controls. This type of risk rating is an example of which of the following?

A. Transferred risk
B. Inherent risk
C. Residual risk

D. Avoided risk

**Answer:** B

**NEW QUESTION 666**
- (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 667**
- (Exam Topic 15)
An organization outgrew its internal data center and is evaluating third-party hosting facilities. In this evaluation, which of the following is a PRIMARY factor for selection?

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

**Answer:** C

**NEW QUESTION 671**
- (Exam Topic 15)
How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

A. It uses clear text and firewall rules.
B. It relies on Virtual Private Networks (VPN).
C. It uses clear text and shared secret keys.
D. It relies on asymmetric encryption keys.

**Answer:** C

**NEW QUESTION 674**
- (Exam Topic 15)
A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to on and security However, an attacker was able to spoof a registered account on the network and query the SAML provider.
What is the MOST common attack leverage against this flaw?

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

**Answer:** A

**NEW QUESTION 677**
- (Exam Topic 15)
Which of the following roles is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications?

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

**Answer:** D

**NEW QUESTION 678**
- (Exam Topic 15)
How is it possible to extract private keys securely stored on a cryptographic smartcard?

A. Bluebugging
B. Focused ion-beam
C. Bluejacking
D. Power analysis

**Answer:** D

**NEW QUESTION 683**
- (Exam Topic 15)

What is the HIGHEST priority in agile development?

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

**Answer:** C


**NEW QUESTION 686**
- (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 688**
- (Exam Topic 15)
An application developer receives a report back from the security team showing their automated tools were able to successfully enter unexpected data into the organization's customer service portal, causing the site to crash. This is an example of which type of testing?

A. Non-functional
B. Positive
C. Performance
D. Negative

**Answer:** D


**NEW QUESTION 691**
- (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 694**
- (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 698**
- (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 700**
- (Exam Topic 15)
When are security requirements the LEAST expensive to implement?

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

**Answer:** D

**NEW QUESTION 705**
- (Exam Topic 15)
Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

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

**Answer:** C


**NEW QUESTION 708**
- (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 709**
- (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 714**
- (Exam Topic 15)
What is the MOST common cause of Remote Desktop Protocol (RDP) compromise?

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

**Answer:** B


**NEW QUESTION 718**
- (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 720**
- (Exam Topic 15)
An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a
per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

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

**Answer:** A


**NEW QUESTION 723**
- (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 728**
- (Exam Topic 15)
Which of the following is a canon of the (ISC)2 Code of Ethics?

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

**Answer:** C


**NEW QUESTION 730**
- (Exam Topic 15)
An organization contracts with a consultant to perform a System Organization Control (SOC) 2 audit on their internal security controls. An auditor documents a finding related to an Application Programming Interface (API) performing an action that is not aligned with the scope or objective of the system. Which trust service principle would be MOST applicable in this situation?

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

**Answer:** B


**NEW QUESTION 732**
- (Exam Topic 15)
What is the MOST appropriate hierarchy of documents when implementing a security program?

A. Organization principle, policy, standard, guideline
B. Policy, organization principle, standard, guideline
C. Standard, policy, organization principle, guideline
D. Organization principle, guideline, policy, standard

**Answer:** C


**NEW QUESTION 735**
- (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 736**
- (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 739**
- (Exam Topic 15)
What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

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

**Answer:** B


**NEW QUESTION 740**
- (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 741
- (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 744
- (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 747
- (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 748
- (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 753
- (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 758
- (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 759

- (Exam Topic 15)
Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

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

**Answer:** D


**NEW QUESTION 763**
- (Exam Topic 15)
The initial security categorization should be done early in the system life cycle and should be reviewed periodically. Why is it important for this to be done correctly?

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

**Answer:** B


**NEW QUESTION 767**
- (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 768**
- (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 773**
- (Exam Topic 15)
What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

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

**Answer:** C


**NEW QUESTION 776**
- (Exam Topic 15)
A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

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

**Answer:** C


**NEW QUESTION 781**
- (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 785**
- (Exam Topic 15)
Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

A. Distributed denial-of-service (DDoS) attack
B. Zero-day attack
C. Phishing attempt
D. Advanced persistent threat (APT) attempt

**Answer:** A


**NEW QUESTION 788**
- (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 793**
- (Exam Topic 15)
A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several 'open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

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

**Answer:** C


**NEW QUESTION 797**
- (Exam Topic 15)
Which of the fallowing statements is MOST accurate regarding information assets?

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

**Answer:** B


**NEW QUESTION 798**
- (Exam Topic 15)
Which of the following is a secure design principle for a new product?

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

**Answer:** A


**NEW QUESTION 803**
- (Exam Topic 15)
What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

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

**Answer:** D


**NEW QUESTION 805**

- (Exam Topic 15)
What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

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

**Answer:** D


**NEW QUESTION 808**
- (Exam Topic 15)
Which of the following system components enforces access controls on an object?

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

**Answer:** B


**NEW QUESTION 809**
- (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 813**
- (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 816**
- (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 820**
- (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 823**
- (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 824**
- (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 828**
......

# Relate Links

**100% Pass Your CISSP Exam with Exambible Prep Materials**

https://www.exambible.com/CISSP-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/