# ISC2

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

**NEW QUESTION 1**
- (Exam Topic 15)
What is the MAIN objective of risk analysis in Disaster Recovery (DR) planning?

A. Establish Maximum Tolerable Downtime (MTD) Information Systems (IS).
B. Define the variable cost for extended downtime scenarios.
C. Identify potential threats to business availability.
D. Establish personnel requirements for various downtime scenarios.

**Answer:** C

**NEW QUESTION 2**
- (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 3**
- (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 4**
- (Exam Topic 15)
Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless
Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

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

**Answer:** B

**NEW QUESTION 5**
- (Exam Topic 15)
A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?
A. Service accounts removal
B. Data validation
C. Logging and monitoring
D. Data sanitization

**Answer:** B

**NEW QUESTION 6**
- (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 7**
- (Exam Topic 15)
A company is planning to implement a private cloud infrastructure. Which of the following recommendations will support the move to a cloud infrastructure?

A. Implement a virtual local area network (VLAN) for each department and create a separate subnet for each VLAN.
B. Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.
C. Implement a virtual local area network (VLAN) to logically separate the local area network (LAN) from the physical switches.

D. implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices and applications.

**Answer:** D

**NEW QUESTION 8**
- (Exam Topic 15)
Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-systems gracefully handle invalid input?

A. Unit testing
B. Integration testing
C. Negative testing
D. Acceptance testing

**Answer:** B

**NEW QUESTION 9**
- (Exam Topic 15)
What is a use for mandatory access control (MAC)?

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

**Answer:** D

**NEW QUESTION 10**
- (Exam Topic 15)
he security organization is loading for a solution that could help them determine with a strong level of confident that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

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

**Answer:** B

**NEW QUESTION 10**
- (Exam Topic 15)
Which of the following is fundamentally required to address potential security issues when initiating software development?

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

**Answer:** C

**NEW QUESTION 11**
- (Exam Topic 15)
An organization has implemented a password complexity and an account lockout policy enforcing five incorrect logins tries within ten minutes. Network users have reported significantly increased account lockouts. Which of the following security principles is this company affecting?

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

**Answer:** A

**NEW QUESTION 16**
- (Exam Topic 15)
A breach investigation …… a website was exploited through an open soured …..Is The FIRB Stan In the Process that could have prevented this breach?

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

**Answer:** B

**NEW QUESTION 17**
- (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 20**
- (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 24**
- (Exam Topic 15)
An organization wants to define its physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

A. Fences eight or more feet high with three strands of barbed wire
B. Fences three to four feet high with a turnstile
C. Fences accompanied by patrolling security guards
D. Fences six to seven feet high with a painted gate

**Answer:** A

**NEW QUESTION 29**
- (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 31**
- (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 35**
- (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 38**
- (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 43**
- (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 45**
- (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 48**
- (Exam Topic 15)
An organization needs a general purpose document to prove that its internal controls properly address security, availability, processing integrity, confidentiality or privacy risks. Which of the following reports is required?

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

**Answer:** C

**NEW QUESTION 53**
- (Exam Topic 15)
An attacker is able to remain indefinitely logged into a exploiting to remain on the web service?

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

**Answer:** C

**NEW QUESTION 57**
- (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 61**
- (Exam Topic 15)
A security practitioner has been asked to model best practices for disaster recovery (DR) and business continuity. The practitioner has decided that a formal committee is needed to establish a business continuity policy. Which of the following BEST describes this stage of business continuity development?

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

**Answer:** D

**NEW QUESTION 63**
- (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 64**
- (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 66**
- (Exam Topic 15)
Which of the following is the MOST effective preventative method to identify security flaws in software?

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

**Answer:** B

**NEW QUESTION 68**
- (Exam Topic 15)
An organization recently upgraded to a Voice over Internet Protocol (VoIP) phone system. Management is concerned with unauthorized phone usage. Security consultant is responsible for putting together a plan to secure these phones. Administrators have assigned unique personal identification number codes for each person in the organization. What is the BEST solution?

A. Use phone locking software to enforce usage and PIN policies.
B. Inform the user to change the PIN regularl
C. Implement call detail records (CDR) reports to track usage.
D. Have the administrator enforce a policy to change the PIN regularl
E. Implement call detail records (CDR) reports to track usage.
F. Have the administrator change the PIN regularl
G. Implement call detail records (CDR) reports to track usage.

**Answer:** C

**NEW QUESTION 70**
- (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 75**
- (Exam Topic 15)
Which of the following is the MOST effective method of detecting vulnerabilities in web-based applications early in the secure Software Development Life Cycle (SDLC)?

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

**Answer:** C

**NEW QUESTION 79**
- (Exam Topic 15)
What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

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

**Answer:** B

**NEW QUESTION 81**
- (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 86**
- (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 87**
- (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 91**
- (Exam Topic 15)
What method could be used to prevent passive attacks against secure voice communications between an organization and its vendor?

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

**Answer:** A

**NEW QUESTION 93**
- (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 95**
- (Exam Topic 15)
Which of the following regulations dictates how data breaches are handled?

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

**Answer:** D

**NEW QUESTION 97**
- (Exam Topic 15)
Which element of software supply chain management has the GREATEST security risk to organizations?

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

**Answer:** B

**NEW QUESTION 102**
- (Exam Topic 15)
A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

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

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

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

**Answer:** A

**NEW QUESTION 106**
- (Exam Topic 15)
Physical Access Control Systems (PACS) allow authorized security personnel to manage and monitor access control for subjects through which function?

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

**Answer:** B

**NEW QUESTION 108**
- (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 109**
- (Exam Topic 15)
Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users internal control over financial reporting?

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

**Answer:** B

**NEW QUESTION 110**
- (Exam Topic 15)
What is the MOST effective response to a hacker who has already gained access to a network and will attempt to pivot to other resources?

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

**Answer:** D

**NEW QUESTION 111**
- (Exam Topic 15)
Which of the following is security control volatility?

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

**Answer:** D

**NEW QUESTION 115**
- (Exam Topic 15)
Which of the following phases in the software acquisition process does developing evaluation criteria take place?

A. Follow-On
B. Planning
C. Contracting
D. Monitoring and Acceptance

**Answer:** D

**NEW QUESTION 118**
- (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 122**
- (Exam Topic 15)
When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

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

**Answer:** C

**NEW QUESTION 126**
- (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 129**
- (Exam Topic 15)
Which of the following are mandatory canons for the (ISC)* Code of Ethics?

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

**Answer:** D

**NEW QUESTION 134**
- (Exam Topic 15)
A developer begins employment with an information technology (IT) organization. On the first day, the developer works through the list of assigned projects and finds that some files within those projects aren't accessible, Other developers working on the same project have no trouble locating and working on the. What is the MOST likely explanation for the discrepancy in access?

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

**Answer:** A

**NEW QUESTION 138**
- (Exam Topic 15)
A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

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

**Answer:** D

**NEW QUESTION 143**
- (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 144**
- (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 145**
- (Exam Topic 15)
Which of the following determines how traffic should flow based on the status of the infrastructure layer?

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

**Answer:** A

**NEW QUESTION 150**
- (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 151**
- (Exam Topic 15)
Which of the following goals represents a modern shift in risk management according to National Institute of Standards and Technology (NIST)?

A. Focus on operating environments that are changing, evolving, and full of emerging threats.
B. Secure information technology (IT) systems that store, process, or transmit organizational information.
C. Enable management to make well-informed risk-based decisions justifying security expenditure.
D. Provide an improved mission accomplishment approach.

**Answer:** C

**NEW QUESTION 156**
- (Exam Topic 15)
Which of the following is the MOST comprehensive Business Continuity (BC) test?

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

**Answer:** C

**NEW QUESTION 160**
- (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 162**
- (Exam Topic 15)
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

A. Provide links to security policies
B. Log all activities associated with sensitive systems
C. Employ strong access controls
D. Confirm that confidentiality agreements are signed

**Answer:** C

**NEW QUESTION 166**
- (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 167**
- (Exam Topic 15)
Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

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

**Answer:** B

**NEW QUESTION 172**
- (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 176**
- (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 181**
- (Exam Topic 15)
Which of the following departments initiates the request, approval, and provisioning business process?

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

**Answer:**

A

**NEW QUESTION 186**
- (Exam Topic 15)
Which one of the following BEST protects vendor accounts that are used for emergency maintenance?

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

**Answer:** B

**NEW QUESTION 188**
- (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 192**
- (Exam Topic 15)
Which of the following is the BEST way to determine the success of a patch management process?

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

**Answer:** A

**NEW QUESTION 195**
- (Exam Topic 15)
Before implementing an internet-facing router, a network administrator ensures that the equipment is baselined/hardened according to approved configurations and settings. This action provides protection against which of the following attacks?

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

**Answer:** B

**NEW QUESTION 198**
- (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 201**
- (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 206**
- (Exam Topic 15)
A federal agency has hired an auditor to perform penetration testing on a critical system as part of the mandatory, annual Federal Information Security Management Act (FISMA) security assessments. The auditor is new to this system but has extensive experience with all types of penetration testing. The auditor has decided to begin with sniffing network traffic. What type of penetration testing is the auditor conducting?

A. White box testing

B. Black box testing
C. Gray box testing
D. Red box testing

**Answer:** C

**NEW QUESTION 210**
- (Exam Topic 15)
In a multi-tenant cloud environment, what approach will secure logical access to assets?

A. Hybrid cloud
B. Transparency/Auditability of administrative access
C. Controlled configuration management (CM)
D. Virtual private cloud (VPC)

**Answer:** D

**NEW QUESTION 212**
- (Exam Topic 15)
After the INITIAL input o f a user identification (ID) and password, what is an authentication system that prompts the user for a different response each time the user logs on?

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

**Answer:** C

**NEW QUESTION 213**
- (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 214**
- (Exam Topic 15)
While classifying credit card data related to Payment Card Industry Data Security Standards (PCI-DSS), which of the following is a PRIMARY security requirement?

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

**Answer:** C

**NEW QUESTION 219**
- (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 221**
- (Exam Topic 15)
A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

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

**Answer:** D

**NEW QUESTION 224**

- (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 225**
- (Exam Topic 15)
Which of the following would be considered an incident if reported by a security information and event management (SIEM) system?

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

**Answer:** C

**NEW QUESTION 226**
- (Exam Topic 15)
Security Software Development Life Cycle (SDLC) expects application code to be written In a consistent manner to allow ease of auditing and which of the following?

A. Protecting
B. Executing
C. Copying
D. Enhancing

**Answer:** A

**NEW QUESTION 230**
- (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 235**
- (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 237**
- (Exam Topic 15)
An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of which of the following types of attack?

A. Cross-Site Scripting (XSS)
B. Cross-site request forgery (CSRF)
C. Injection
D. Click jacking

**Answer:** B

**NEW QUESTION 239**
- (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 242**
- (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 244**
- (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 249**
- (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 252**
- (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 257**
- (Exam Topic 15)
Which of the following is the PRIMARY goal of logical access controls?

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

**Answer:** C

**NEW QUESTION 258**
- (Exam Topic 15)
Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

A. Sniffing the traffic of a compromised host inside the network
B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network
C. A brute force password attack on the Secure Shell (SSH) port of the controller
D. Remote Authentication Dial-In User Service (RADIUS) token replay attack

**Answer:** B

**NEW QUESTION 261**
- (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 266**
- (Exam Topic 15)
Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

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

**Answer:** B

**NEW QUESTION 270**
- (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 275**
- (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 277**
- (Exam Topic 15)
Which of the following types of web-based attack is happening when an attacker is able to send a well-crafted, malicious request to an authenticated user without the user realizing it?

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

**Answer:** B

**NEW QUESTION 280**
- (Exam Topic 15)
Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

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

**Answer:** B

**NEW QUESTION 282**
- (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 285**
- (Exam Topic 15)
Which of the following explains why classifying data is an important step in performing a Risk assessment?

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

**Answer:** D

**NEW QUESTION 287**
- (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 292**
- (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 294**
- (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 297**
- (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 299**
- (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 303**
- (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 307**
- (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 309**
- (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 310**
- (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 313**
- (Exam Topic 15)
Which of the following BEST describes why software assurance is critical in helping prevent an increase in business and mission risk for an organization?

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

**Answer:** B

**NEW QUESTION 317**
- (Exam Topic 15)
What is the MOST important factor in establishing an effective Information Security Awareness Program?

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

**Answer:** C

**NEW QUESTION 321**
- (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 322**
- (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 327**
- (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 332**
- (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 336**
- (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 340**
- (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 341**
- (Exam Topic 15)
Which of the following attack types can be used to compromise the integrity of data during transmission?

A. Keylogging
B. Packet sniffing
C. Synchronization flooding
D. Session hijacking

**Answer:** B

**NEW QUESTION 346**
- (Exam Topic 15)
The security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network. Which solution is MOST effective at discovering a successful network breach?

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

**Answer:** A

**NEW QUESTION 350**

- (Exam Topic 15)
A Chief Information Officer (CIO) has delegated responsibility of their system security to the head of the information technology (IT) department. While corporate policy dictates that only the CIO can make decisions on the level of data protection required, technical implementation decisions are done by the head of the IT department. Which of the following BEST describes the security role filled by the head of the IT department?

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

**Answer:** D

**NEW QUESTION 355**
- (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 357**
- (Exam Topic 15)
Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

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

**Answer:** C

**NEW QUESTION 359**
- (Exam Topic 15)
Which of the following is the MOST important first step in preparing for a security audit?

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

**Answer:** B

**NEW QUESTION 360**
- (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 365**
- (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 366**
- (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.

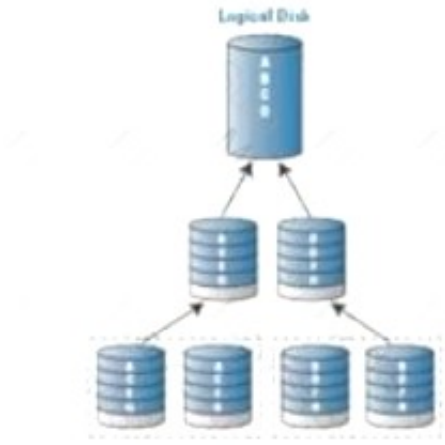
**Answer:** D

**NEW QUESTION 369**
- (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 370**
- (Exam Topic 15)
Which Redundant Array c/ Independent Disks (RAID) Level does the following diagram represent?




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

**Answer:** D

**NEW QUESTION 372**
- (Exam Topic 15)
The MAIN purpose of placing a tamper seal on a computer system's case is to:

A. raise security awareness.
B. detect efforts to open the case.
C. expedite physical auditing.
D. make it difficult to steal internal components.

**Answer:** A

**NEW QUESTION 375**
- (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 380**
- (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 385**
- (Exam Topic 15)
Secure coding can be developed by applying which one of the following?

A. Applying the organization's acceptable use guidance
B. Applying the industry best practice coding guidelines
C. Applying rapid application development (RAD) coding

D. Applying the organization's web application firewall (WAF) policy

**Answer:** B

**NEW QUESTION 389**
- (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 393**
- (Exam Topic 15)
Which of the following vulnerabilities can be BEST detected using automated analysis?

A. Valid cross-site request forgery (CSRF) vulnerabilities
B. Multi-step process attack vulnerabilities
C. Business logic flaw vulnerabilities
D. Typical source code vulnerabilities

**Answer:** D

**NEW QUESTION 396**
- (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 401**
- (Exam Topic 15)
A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

A. Validate passwords using a stored procedure.
B. Allow only the application to have access to the password field in order to verify user authentication.
C. Use a salted cryptographic hash of the password.
D. Encrypt the entire database and embed an encryption key in the application.

**Answer:** C

**NEW QUESTION 406**
- (Exam Topic 15)
Which of the following is the MOST important consideration in selecting a security testing method based on different Radio-Frequency Identification (RFID) vulnerability types?

A. The performance and resource utilization of tools
B. The quality of results and usability of tools
C. An understanding of the attack surface
D. Adaptability of testing tools to multiple technologies

**Answer:** C

**NEW QUESTION 409**
- (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 412**
- (Exam Topic 15)
Which of the following technologies can be used to monitor and dynamically respond to potential threats on web applications?

A. Security Assertion Markup Language (SAML)
B. Web application vulnerability scanners
C. Runtime application self-protection (RASP)
D. Field-level tokenization

**Answer:** C

**NEW QUESTION 417**
- (Exam Topic 15)
Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

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

**Answer:** A

**NEW QUESTION 421**
- (Exam Topic 15)
Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

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

**Answer:** A

**NEW QUESTION 425**
- (Exam Topic 15)
A Certified Information Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to4 perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)? Code of Professional Ethics, which of the following should the CISSP do?

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

**Answer:** C

**NEW QUESTION 426**
- (Exam Topic 15)
Which of the following is the BEST method to gather evidence from a computer's hard drive?

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

**Answer:** D

**NEW QUESTION 429**
- (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 431**
- (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 435**

- (Exam Topic 15)
A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

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

**Answer:** B

**NEW QUESTION 438**
- (Exam Topic 15)
Which of the following is a security weakness in the evaluation of common criteria (CC) products?

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

**Answer:** A

**NEW QUESTION 439**
- (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 441**
- (Exam Topic 15)
What is the PRIMARY objective of the post-incident phase of the incident response process in the security operations center (SOC)?

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

**Answer:** A

**NEW QUESTION 443**
- (Exam Topic 15)
A security professional can BEST mitigate the risk of using a Commercial Off-The-Shelf (COTS) solution by deploying the application with which of the following controls in ?

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

**Answer:** A

**NEW QUESTION 448**
- (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 450**
- (Exam Topic 15)
Which of the following techniques evaluates the secure Bet principles of network or software architectures?

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

**Answer:** A

**NEW QUESTION 451**
- (Exam Topic 15)
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 453**
- (Exam Topic 15)
A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to on and security However, an attacker was able to spoof a registered account on the network and query the SAML provider.
What is the MOST common attack leverage against this flaw?

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

**Answer:** A

**NEW QUESTION 458**
- (Exam Topic 15)
Which of the following is the MOST effective corrective control to minimize the effects of a physical intrusion?

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

**Answer:** C

**NEW QUESTION 461**
- (Exam Topic 15)
Which of the following BEST describes centralized identity management?

A. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
B. Service providers agree to integrate identity system recognition across organizational boundaries.
C. Service providers identify an entity by behavior analysis versus an identification factor.
D. Service providers perform as both the credential and identity provider (IdP).

**Answer:** B

**NEW QUESTION 466**
- (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 467**
- (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 471**
- (Exam Topic 15)
Which of the following contributes MOST to the effectiveness of a security officer?

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

**Answer:** A

**NEW QUESTION 474**
- (Exam Topic 15)
Which of the following is an important design feature for the outer door o f a mantrap?

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

**Answer:** D

**NEW QUESTION 479**
- (Exam Topic 15)
A company-wide penetration test result shows customers could access and read files through a web browser. Which of the following can be used to mitigate this vulnerability?

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

**Answer:** B

**NEW QUESTION 481**
- (Exam Topic 15)
Which of the following is a covert channel type?

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

**Answer:** A

**NEW QUESTION 482**
- (Exam Topic 15)
Which of the following activities should a forensic examiner perform FIRST when determining the priority of digital evidence collection at a crime scene?

A. Gather physical evidence,
B. Establish order of volatility.
C. Assign responsibilities to personnel on the scene.
D. Establish a list of files to examine.

**Answer:** C

**NEW QUESTION 485**
- (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 490**
- (Exam Topic 15)
What type of risk is related to the sequences of value-adding and managerial activities undertaken in an organization?

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

**Answer:** B

**NEW QUESTION 491**
- (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 493**
- (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 496**
- (Exam Topic 15)
A hospital's building controls system monitors and operates the environmental equipment to maintain a safe and comfortable environment. Which of the following could be
used to minimize the risk of utility supply interruption?

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

**Answer:** D

**NEW QUESTION 497**
- (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 500**
- (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 504**
- (Exam Topic 15)
What is the PRIMARY purpose of auditing, as it relates to the security review cycle?

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

**Answer:** A

**NEW QUESTION 509**
- (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 513**

- (Exam Topic 15)
When MUST an organization's information security strategic plan be reviewed?

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

**Answer:** D

**NEW QUESTION 517**
- (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 520**
- (Exam Topic 15)
Which of the following techniques evaluates the secure design principles of network OF software architectures?

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

**Answer:** B

**NEW QUESTION 521**
- (Exam Topic 15)
How does Radio-Frequency Identification (RFID) assist with asset management?

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

**Answer:** B

**NEW QUESTION 526**
- (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 530**
- (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 534**
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

**Answer:** C

**NEW QUESTION 536**
- (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 538**
- (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 539**
- (Exam Topic 15)
In an IDEAL encryption system, who has sole access to the decryption key?

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

**Answer:** B

**NEW QUESTION 543**
- (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 545**
- (Exam Topic 15)
The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

A. biometric data cannot be changed.
B. Separate biometric data streams require increased security.
C. The biometric devices are unknown.
D. Biometric data must be protected from disclosure.

**Answer:** A

**NEW QUESTION 547**
- (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 552**
- (Exam Topic 15)
Which of the following are all elements of a disaster recovery plan (DRP)?

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

**Answer:** C

**NEW QUESTION 553**
- (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 558**
- (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 562**
- (Exam Topic 15)
Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

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

**Answer:** B

**NEW QUESTION 563**
- (Exam Topic 14)
Which of the following are core categories of malicious attack against Internet of Things (IOT) devices?

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

**Answer:** D

**NEW QUESTION 565**
- (Exam Topic 14)
In a dispersed network that lacks central control, which of the following is die PRIMARY course of action to mitigate exposure?

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

**Answer:** C

**NEW QUESTION 568**
- (Exam Topic 14)
When developing the entitlement review process, which of the following roles is responsible for determining who has a need for the information?

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

**Answer:** B

**NEW QUESTION 570**
- (Exam Topic 14)
Which one of the following documentation should be included in a Disaster Recovery (DR) package?

A. Source code, compiled code, firmware updates, operational log book and manuals.
B. Data encrypted in original format, auditable transaction data, and recovery instructions for future extraction on demand.
C. Hardware configuration instructions, hardware configuration software, an operating system image, a data restoration option, media retrieval instructions,…..

D. System configuration including hardware, software, hardware, interfaces, software Application Programming Interface (API) configuration, data structure, ….

**Answer:** C

**NEW QUESTION 573**
- (Exam Topic 14)
Which of the following entails identification of data end links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

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

**Answer:** A

**NEW QUESTION 576**
- (Exam Topic 14)
What type of access control determines the authorization to resource based on pre-defined job titles within an organization?

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

**Answer:** A

**NEW QUESTION 577**
- (Exam Topic 14)
An organization wants to enable uses to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (F1M). Which of the following is used behind the scenes in a FIM deployment?

A. Standard Generalized Markup Language (SGML)
B. Extensible Markup Language (XML)
C. Security Assertion Markup Language (SAML)
D. Transaction Authority Markup Language (XAML)

**Answer:** C

**NEW QUESTION 581**
- (Exam Topic 14)
Continuity of operations is BEST supported by which of the following?

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

**Answer:** B

**NEW QUESTION 584**
- (Exam Topic 14)
For the purpose of classification, which of the following is used to divide trust domain and trust boundaries?

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

**Answer:** A

**NEW QUESTION 589**
- (Exam Topic 14)
If a content management system (CMC) is implemented, which one of the following would occur?

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

**Answer:** D

**NEW QUESTION 594**
- (Exam Topic 14)
Physical assets defined in an organization’s Business Impact Analysis (BIA) could include which of the following?

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

**Answer:** B

**NEW QUESTION 596**
- (Exam Topic 14)
Which of the following is a characteristic of the independent testing of a program?

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

**Answer:** A

**NEW QUESTION 601**
- (Exam Topic 14)
Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities?

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

**Answer:** C

**NEW QUESTION 604**
- (Exam Topic 14)
Which of the following is the GREATEST security risk associated with the user of identity as a service (IDaaS) when an organization its own software?

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

**Answer:** B

**NEW QUESTION 609**
- (Exam Topic 14)
Which of the following is a MAJOR concern when there is a need to preserve or retain information for future retrieval?

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

**Answer:** C

**NEW QUESTION 611**
- (Exam Topic 14)
Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?

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

**Answer:** D

**NEW QUESTION 614**
- (Exam Topic 14)

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

**Answer:** D

**NEW QUESTION 616**
- (Exam Topic 14)

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

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

**Answer:** B

**NEW QUESTION 619**
- (Exam Topic 14)
When adopting software as a service (Saas), which security responsibility will remain with remain with the adopting organization?

A. Physical security
B. Data classification
C. Network control
D. Application layer control

**Answer:** B

**NEW QUESTION 622**
- (Exam Topic 14)
A security practitioner has been tasked with establishing organizational asset handling procedures. What should be considered that would have the GRFATEST impact to the development of these procedures?

A. Media handling procedures
B. User roles and responsibilities
C. Acceptable Use Policy (ALP)
D. Information classification scheme

**Answer:** D

**NEW QUESTION 623**
- (Exam Topic 14)
Which of the following is the MOST important reason for using a chain of custody from?

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

**Answer:** A

**NEW QUESTION 627**
- (Exam Topic 14)
What is the PRIMARY purpose for an organization to conduct a security audit?

A. To ensure the organization is adhering to a well-defined standard
B. To ensure the organization is applying security controls to mitigate identified risks
C. To ensure the organization is configuring information systems efficiently
D. To ensure the organization is documenting findings

**Answer:** A

**NEW QUESTION 631**
- (Exam Topic 14)
When should an application invoke re-authentication in addition to initial user authentication?

A. At the application sign-off
B. Periodically during a session
C. After a period of inactivity
D. For each business process

**Answer:** C

**NEW QUESTION 635**
- (Exam Topic 14)
Which is the RECOMMENDED configuration mode for sensors for an intrusion prevention system (IPS) if the prevention capabilities will be used?

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

**Answer:** C

**NEW QUESTION 636**
- (Exam Topic 14)
An organization that has achieved a Capability Maturity model Integration (CMMI) level of 4 has done which of the following?

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

**Answer:** C

**NEW QUESTION 640**
- (Exam Topic 14)
Which layer of the Open system Interconnect (OSI) model is responsible for secure data transfer between applications, flow control, and error detection and correction?

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

**Answer:** B

**NEW QUESTION 645**
- (Exam Topic 14)
Which of the following job functions MUST be separated to maintain data and application integrity?

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

**Answer:** D

**NEW QUESTION 647**
- (Exam Topic 14)
Which of the following is the BEST defense against password guessing?

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

**Answer:** D

**NEW QUESTION 651**
- (Exam Topic 14)
Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?

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

**Answer:** B

**NEW QUESTION 652**
- (Exam Topic 14)
A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

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

**Answer:** B

**NEW QUESTION 657**
- (Exam Topic 14)
Which layer of the Open systems Interconnection (OSI) model is being targeted in the event of a Synchronization (SYN) flood attack?

A. Session
B. Transport
C. Network

D. Presentation

**Answer:** B

**NEW QUESTION 659**
- (Exam Topic 14)
What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

A. Business Impact Analysis (BIA)
B. Security Assessment Report (SAR)
C. Plan of Action and Milestones {POA&M)
D. Security Assessment Plan (SAP)

**Answer:** C

**NEW QUESTION 660**
- (Exam Topic 14)
How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

A. Use a Virtual Local Area Network (VLAN) to segment the network
B. Implement a bastion host
C. Install anti-virus on all enceinte
D. Enforce port security on access switches

**Answer:** A

**NEW QUESTION 665**
- (Exam Topic 14)
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

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

**Answer:** C

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

**NEW QUESTION 667**
- (Exam Topic 14)
A new Chief Information Officer (CIO) created a group to write a data retention policy based on applicable laws. Which of the following is the PRIMARY motivation for the policy?

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

**Answer:** B

**NEW QUESTION 669**
- (Exam Topic 14)
In fault-tolerant systems, what do rollback capabilities permit?

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

**Answer:** A

**NEW QUESTION 673**
- (Exam Topic 14)
What is the BEST way to correlate large volumes of disparate data sources in a Security Operations Center (SOC) environment?

A. Implement Intrusion Detection System (IDS).
B. Implement a Security Information and Event Management (SIEM) system.
C. Hire a team of analysts to consolidate data and generate reports.
D. Outsource the management of the SOC.

**Answer:** B

**NEW QUESTION 678**
- (Exam Topic 14)
When deploying en Intrusion Detection System (IDS) on a high-volume network, the need to distribute the load across multiple sensors would create which technical problem?

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

**Answer:** A

**NEW QUESTION 680**
- (Exam Topic 14)
Which of the following authorization standards is built to handle Application programming Interface (API) access for federated Identity management (FIM)?

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

**Answer:** C

**NEW QUESTION 681**
- (Exam Topic 14)
Digital certificates used transport Layer security (TLS) support which of the following?

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

**Answer:** A

**NEW QUESTION 682**
- (Exam Topic 14)
When a system changes significantly, who is PRIMARILY responsible for assessing the security impact?

A. Chief Information Security Officer (CISO)
B. Information System Owner
C. Information System Security Officer (ISSO)
D. Authorizing Official

**Answer:** B

**NEW QUESTION 683**
- (Exam Topic 14)
Which of the following is a characteristic of a challenge/response authentication process?

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

**Answer:** A

**NEW QUESTION 685**
- (Exam Topic 14)
A security engineer is designing a Customer Relationship Management (CRM) application for a third-party vendor. In which phase of the System Development Life Cycle (SDLC) will it be MOST beneficial to conduct a data sensitivity assessment?

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

**Answer:** B

**NEW QUESTION 689**
- (Exam Topic 14)
What is the MAIN reason to ensure the appropriate retention periods are enforced for data stored on electronic media?

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

**Answer:** D

**NEW QUESTION 693**
- (Exam Topic 14)
Which of the following technologies would provide the BEST alternative to anti-malware software?

A. Host-based Intrusion Detection Systems (HIDS)
B. Application whitelisting
C. Host-based firewalls
D. Application sandboxing

**Answer:** B

**NEW QUESTION 696**
- (Exam Topic 14)
Which of the following media is least problematic with data remanence?

A. Magnetic disk
B. Electrically Erasable Programming read-only Memory (EEPROM)
C. Dynamic Random Access Memory (DRAM)
D. Flash memory

**Answer:** C

**NEW QUESTION 701**
- (Exam Topic 14)
An organization is required to comply with the Payment Card Industry Data Security Standard (PCI-DSS), what is the MOST effective approach to safeguard digital and paper media that contains cardholder data?

A. Use and regularity update antivirus software.
B. Maintain strict control over storage of media
C. Mandate encryption of cardholder data.
D. Configure firewall rules to protect the data.

**Answer:** C

**NEW QUESTION 703**
- (Exam Topic 14)
After a breach incident, investigators narrowed the attack to a specific network administrator's credentials. However, there was no evidence to determine how the hackers obtained the credentials. Much of the following actions could have BEST avoided the above breach per the investigation described above?

A. A periodic review of network access loos
B. A periodic review of active users en the network
C. A periodic review of all privileged accounts actions
D. A periodic review of password strength of all users across the organization

**Answer:** C

**NEW QUESTION 705**
- (Exam Topic 14)
Which of the following provides the GREATEST level of data security for a Virtual Private Network (VPN) connection?

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

**Answer:** B

**NEW QUESTION 707**
- (Exam Topic 14)
Change management policies and procedures belong to which of the following types of controls?

A. Directive
B. Detective
C. Corrective
D. Preventative

**Answer:** A

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

**NEW QUESTION 708**
- (Exam Topic 14)

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

A. Review all security policies and procedures.
B. Ensure staff is trained in security.
C. Determine if you need to conduct a full security assessment.
D. Evaluate the problems identified in the test result.

**Answer:** D

**NEW QUESTION 709**
- (Exam Topic 14)
Which of the following steps should be conducted during the FIRST phase of software assurance in a generic acquisition process?

A. Establishing and consenting to the contract work schedule
B. Issuing a Request for proposal (RFP) with a work statement
C. Developing software requirements to be included in work statement
D. Reviewing and accepting software deliverables

**Answer:** C

**NEW QUESTION 710**
- (Exam Topic 14)
Information security metrics provide the GREATEST value tp management when based upon the security manager’s knowledge of which of the following?

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

**Answer:** B

**NEW QUESTION 715**
- (Exam Topic 14)
Which of the following is the PRIMARY security consideration for how an organization should handle Information Technology (IT) assets?

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

**Answer:** D

**NEW QUESTION 717**
- (Exam Topic 14)
What high Availability (HA) option of database allows multiple clients to access multiple database servers simultaneously?

A. Non-Structured Query Language (NoSQL) database
B. Relational database
C. Shadow database
D. Replicated database

**Answer:** C

**NEW QUESTION 722**
- (Exam Topic 14)
Which security architecture strategy could be applied to secure an operating system (OS) baseline for deployment within the corporate enterprise?

A. Principle of Least Privilege
B. Principle of Separation of Duty
C. Principle of Secure Default
D. principle of Fail Secure

**Answer:** D

**NEW QUESTION 724**
- (Exam Topic 14)
Which of the following trust services principles refers to the accessibility of information used by the systems, products, or services offered to a third-party provider’s customers?

A. Security
B. Privacy
C. Access
D. Availability

**Answer:** C

**Explanation:**

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

**NEW QUESTION 727**
- (Exam Topic 14)
Which of the following is the BEST way to protect against structured Query language (SQL) injection?

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

**Answer:** D

**NEW QUESTION 730**
- (Exam Topic 14)
Which one of the following would cause an immediate review and possible change to the security policies of an organization?

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

**Answer:** D

**NEW QUESTION 731**
- (Exam Topic 14)
Which of the following MUST an organization do to effectively communicate is security strategy to all affected parties?

A. Involve representatives from each key organizational area.
B. Provide regular updates to the board of directors.
C. Notify staff of changes to the strategy.
D. Remove potential communication barriers.

**Answer:** C

**NEW QUESTION 733**
- (Exam Topic 14)
Which of the following techniques is MOST useful when dealing with Advanced persistent Threat (APT) intrusions on live virtualized environments?

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

**Answer:** B

**NEW QUESTION 736**
- (Exam Topic 14)
An Intrusion Detection System (IDS) is based on the general hypothesis that a security violation is associated with a pattern of system usage which can be

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

**Answer:** A

**NEW QUESTION 739**
- (Exam Topic 14)
Which of the following is MOST important when determining appropriate countermeasures for an identified risk?

A. Interaction with existing controls
B. Cost
C. Organizational risk tolerance
D. Patch availability

**Answer:** C

**NEW QUESTION 740**
- (Exam Topic 14)
Which of the following is the MOST significant benefit to implementing a third-party federated identity architecture?

A. Attribute assertions as agencies can request a larger set of attributes to fulfill service delivery
B. Data decrease related to storing personal information
C. Reduction in operational costs to the agency
D. Enable business objectives so departments can focus on mission rather than the business of identitymanagement

**Answer:** C

**NEW QUESTION 744**
- (Exam Topic 14)
Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

A. Security credentials
B. Known vulnerabilities
C. Inefficient algorithms
D. Coding mistakes

**Answer:** A

**NEW QUESTION 748**
- (Exam Topic 14)
How does identity as a service (IDaaS) provide an easy mechanism for integrating identity service into individual applications with minimal development effort?

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

**Answer:** D

**NEW QUESTION 750**
- (Exam Topic 14)
What is the threat modeling order using process for Attack simu-lation and threat analysis (PASTA)?

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

**Answer:** A

**NEW QUESTION 753**
- (Exam Topic 14)
Which of the following should be included in a hardware retention policy? Which of the following should be included in a hardware retention policy?

A. The use of encryption technology to encrypt sensitive data prior to retention
B. Retention of data for only one week and outsourcing the retention to a third-party vendor
C. Retention of all sensitive data on media and hardware
D. A plan to retain data required only for business purposes and a retention schedule

**Answer:** A

**NEW QUESTION 758**
- (Exam Topic 14)
Which of the following needs to be taken into account when assessing vulnerability?

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

**Answer:** A

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

**NEW QUESTION 763**
- (Exam Topic 14)
Which of the following is the key requirement for test results when implementing forensic procedures?

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

**Answer:** B

**NEW QUESTION 767**
- (Exam Topic 14)
An Internet software application requires authentication before a user is permitted to utilize the resource. Which testing scenario BEST validates the functionality of the application?

A. Reasonable data testing
B. Input validation testing
C. Web session testing
D. Allowed data bounds and limits testing

**Answer:** B

**NEW QUESTION 768**
- (Exam Topic 14)
Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

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

**Answer:** C

**NEW QUESTION 769**
- (Exam Topic 14)
Which of the following techniques BEST prevents buffer overflows?

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

**Answer:** B

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

**NEW QUESTION 770**
- (Exam Topic 14)
Which attack defines a piece of code that is inserted into software to trigger a malicious function?

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

**Answer:** D

**NEW QUESTION 774**
- (Exam Topic 14)
Which of the following in the BEST way to reduce the impact of an externally sourced flood attack?

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

**Answer:** A

**NEW QUESTION 775**
- (Exam Topic 14)
Which inherent password weakness does a One Time Password (OTP) generator overcome?

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

**Answer:** D

**NEW QUESTION 780**
- (Exam Topic 14)
Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information form malicious software?

A. Analyze the behavior of the program.
B. Examine the file properties and permissions.
C. Review the code to identify its origin.
D. Analyze the logs generated by the software.

**Answer:** A

**NEW QUESTION 783**
- (Exam Topic 14)
Which testing method requires very limited or no information about the network infrastructure?

A. While box
B. Static
C. Black box
D. Stress

**Answer:** C

**NEW QUESTION 784**
- (Exam Topic 14)
A client has reviewed a vulnerability assessment report and has stated it is inaccurate. The client states that the vulnerabilities listed are not valid because the host's Operating system (OS) was not properly detected.
Where in the vulnerability assessment process did the error MOST likely occur?

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

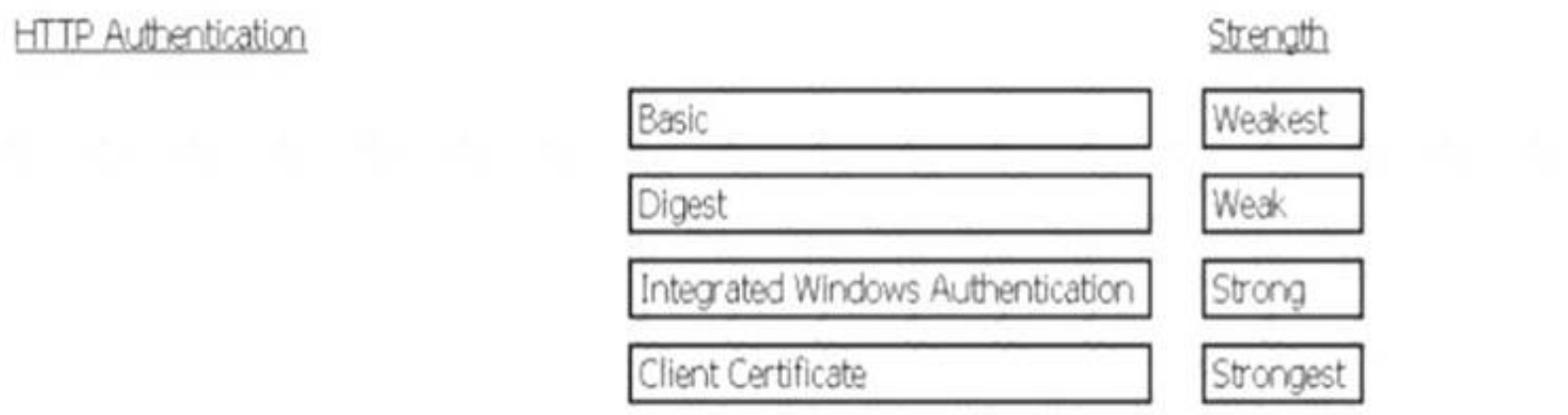
**Answer:** A

**NEW QUESTION 785**
- (Exam Topic 14)
Rank the Hypertext Transfer protocol (HTTP) authentication types shows below in order of relative strength. Drag the authentication type on the correct positions on the right according to strength from weakest to
strongest.


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 789**
- (Exam Topic 14)
For a federated identity solution, a third-party Identity Provider (IdP) is PRIMARILY responsible for which of the following?

A. Access Control
B. Account Management
C. Authentication
D. Authorization

**Answer:** C

**NEW QUESTION 794**
- (Exam Topic 14)
In the common criteria (CC) for information technology (IT) security evaluation, increasing Evaluation Assurance Levels (EAL) results in which of the following?

A. Increased functionality
B. Increased interoperability
C. Increase in resource requirement
D. Increase in evaluated systems

**Answer:** B

**NEW QUESTION 796**
- (Exam Topic 14)
Which of the following is critical if an empolyee is dismissed due to violation of an organization's acceptable use policy (Aup) ?

A. Appropriate documentation
B. privilege suspension
C. proxy records
D. Internet access logs

**Answer:** A

**NEW QUESTION 800**
- (Exam Topic 14)
What determines the level of security of a combination lock?

A. Complexity of combination required to open the lock
B. Amount of time it takes to brute force the combination
C. The number of barrels associated with the internal mechanism
D. The hardness score of the metal lock material

**Answer:** A

**Explanation:**
Reference:
https://books.google.com.pk/books?id=RbihG-YALUkC&pg=PA976&lpg=PA976&dq=CISSP+determines+the

**NEW QUESTION 801**
- (Exam Topic 14)
Which of the following is critical if an employee is dismissed due to violation of an organization's Acceptable Use Policy (ALP)?

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

**Answer:** B

**NEW QUESTION 805**
- (Exam Topic 14)
Which of the following attributes could be used to describe a protection mechanism of an open design methodology?

A. lt must be tamperproof to protect it from malicious attacks.
B. It can facilitate independent confirmation of the design security.
C. It can facilitate blackbox penetration testing.
D. It exposes the design to vulnerabilities and malicious attacks.

**Answer:** A

**NEW QUESTION 809**
- (Exam Topic 14)
Secure real-time transport protocol (SRTP) provides security for which of the following?

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

**Answer:** B

**NEW QUESTION 814**
- (Exam Topic 14)
Which of the following BEST describes the responsibilities of data owner?

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

**Answer:** B

**NEW QUESTION 816**
- (Exam Topic 14)
Which of the following processes has the PRIMARY purpose of identifying outdated software versions, missing patches, and lapsed system updates?

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

**Answer:** B

**Explanation:**
Reference:
https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/vulnerab

**NEW QUESTION 820**
- (Exam Topic 14)
What is the BEST way to establish identity over the internet?

A. Challenge Handshake Authentication Protocol (CHAP) and strong passwords
B. Internet Mail Access Protocol (IMAP) with Triple Data Encryption Standard (3DES)
C. Remote Authentication Dial-In User Service (RADIUS) server with hardware tokens
D. Remote user authentication via Simple Object Access Protocol (SOAP)

**Answer:** D

**NEW QUESTION 821**
- (Exam Topic 14)
What is the most effective form of media sanitization to ensure residual data cannot be retrieved?

A. Clearing
B. Destroying
C. Purging
D. Disposal

**Answer:** B

**NEW QUESTION 824**
- (Exam Topic 13)
Which one of the following is an advantage of an effective release control strategy form a configuration control standpoint?

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

**Answer:** A

**NEW QUESTION 827**
- (Exam Topic 13)
Access to which of the following is required to validate web session management?

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

**Answer:** B

**NEW QUESTION 832**
- (Exam Topic 13)
A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report.
In which phase of the assessment was this error MOST likely made?

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

**Answer:** A

**Explanation:**
Section: Security Assessment and Testing

**NEW QUESTION 834**

- (Exam Topic 13)
Who is responsible for the protection of information when it is shared with or provided to other organizations?

A. Systems owner
B. Authorizing Official (AO)
C. Information owner
D. Security officer

**Answer:** C

**Explanation:**
Section: Security Operations

**NEW QUESTION 836**
- (Exam Topic 13)
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

A. To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
B. To validate backup sites' effectiveness
C. To find out what does not work and fix it
D. To create a high level DRP awareness among Information Technology (IT) staff

**Answer:** B

**NEW QUESTION 837**
- (Exam Topic 13)
Who would be the BEST person to approve an organizations information security policy?

A. Chief Information Officer (CIO)
B. Chief Information Security Officer (CISO)
C. Chief internal auditor
D. Chief Executive Officer (CEO)

**Answer:** B

**Explanation:**
Section: Security Operations

**NEW QUESTION 842**
- (Exam Topic 13)
Which of the following is a common feature of an Identity as a Service (IDaaS) solution?

A. Single Sign-On (SSO) authentication support
B. Privileged user authentication support
C. Password reset service support
D. Terminal Access Controller Access Control System (TACACS) authentication support

**Answer:** A

**NEW QUESTION 846**
- (Exam Topic 13)
Which of the following combinations would MOST negatively affect availability?

A. Denial of Service (DoS) attacks and outdated hardware
B. Unauthorized transactions and outdated hardware
C. Fire and accidental changes to data
D. Unauthorized transactions and denial of service attacks

**Answer:** A

**NEW QUESTION 848**
- (Exam Topic 13)
What capability would typically be included in a commercially available software package designed for access control?

A. Password encryption
B. File encryption
C. Source library control
D. File authentication

**Answer:** A

**NEW QUESTION 853**
- (Exam Topic 13)
Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

A. Memory review

B. Code review
C. Message division
D. Buffer division

**Answer:** B

**NEW QUESTION 858**
- (Exam Topic 13)
What is the PRIMARY goal of fault tolerance?

A. Elimination of single point of failure
B. Isolation using a sandbox
C. Single point of repair
D. Containment to prevent propagation

**Answer:** A

**NEW QUESTION 863**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

## CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

* CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year