Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

https://www.2passeasy.com/dumps/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)
An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

A. Deduplication
B. Compression
C. Replication
D. Caching

Answer: B

NEW QUESTION 3
- (Exam Topic 15)
Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

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

Answer: C

NEW QUESTION 4
- (Exam Topic 15)
Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

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

Answer: B

NEW QUESTION 5
- (Exam Topic 15)
The security architect is designing and implementing an internal certification authority to generate digital certificates for all employees. Which of the following is the BEST solution to securely store the private keys?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 15)
Wireless users are reporting intermittent Internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time.
The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client's wireless settings.
C. Confirm that a valid passphrase is being used during the web authentication.
D. Investigate for a client's disassociation caused by an evil twin AP

Answer: A

NEW QUESTION 7
- (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 8
- (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 9
- (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 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)
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 13
- (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 is the FIRST step for defining Service Level Requirements (SLR)?

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

Answer: D

NEW QUESTION 22
- (Exam Topic 15)
During a penetration test, what are the three PRIMARY objectives of the planning phase?

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

Answer: D

NEW QUESTION 25
- (Exam Topic 15)
A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

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

Answer: C

NEW QUESTION 27
- (Exam Topic 15)
Which of the following ensures old log data is not overwritten?

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

Answer: D

NEW QUESTION 28
- (Exam Topic 15)
In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed?

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

Answer: D

NEW QUESTION 32
- (Exam Topic 15)
To minimize the vulnerabilities of a web-based application, which of the following FIRST actions will lock down the system and minimize the risk of an attack?

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

Answer: D

NEW QUESTION 36
- (Exam Topic 15)
When reviewing the security logs, the password shown for an administrative login event was ' OR ' '1'='1' --. This is an example of which of the following kinds of attack?

A. Brute Force Attack
B. Structured Query Language (SQL) Injection
C. Cross-Site Scripting (XSS)
D. Rainbow Table Attack

Answer: B

NEW QUESTION 38
- (Exam Topic 15)
In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to the resource’s access to the production operating system (OS) directory structure?

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

C. From Administrator privileges to No Access privileges
D. From No Access Privileges to Author privileges

Answer: C

NEW QUESTION 41
- (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 45
- (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 47
- (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 52
- (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 54
- (Exam Topic 15)
Information security practitioners are in the midst of implementing a new firewall. Which of the following failure methods would BEST prioritize security in the event of failure?

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

Answer: A

NEW QUESTION 57
- (Exam Topic 15)
What would be the BEST action to take in a situation where collected evidence was left unattended overnight in an unlocked vehicle?

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

Answer: D

NEW QUESTION 59
- (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 62
- (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 66
- (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 67
- (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 72
- (Exam Topic 15)
Which audit type is MOST appropriate for evaluating the effectiveness of a security program?

A. Threat
B. Assessment
C. Analysis
D. Validation

Answer: B

NEW QUESTION 74
- (Exam Topic 15)
A user is allowed to access the file labeled “Financial Forecast,” but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

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

Answer: B

NEW QUESTION 79
- (Exam Topic 15)
Which of the following types of firewall only examines the “handshaking” between packets before forwarding traffic?

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

Answer: C

NEW QUESTION 80
- (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 84
- (Exam Topic 15)
What type of investigation applies when malicious behavior is suspected between two organizations?

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

Answer: A

NEW QUESTION 89
- (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 91
- (Exam Topic 15)
Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

A. Isolate the network, log an independent report, fix the problem, and redeploy the computer.
B. Isolate the network, install patches, and report the occurrence.
C. Prioritize, report, and investigate the occurrence.
D. Turn the rooter off, perform forensic analysis, apply the appropriate fin, and log incidents.

Answer: C

NEW QUESTION 93
- (Exam Topic 15)
Which of the following is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions?

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

Answer: D

NEW QUESTION 95
- (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 96
- (Exam Topic 15)
The disaster recovery (DR) process should always include

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

Answer:

A

NEW QUESTION 100
- (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 102
- (Exam Topic 15)
Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

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

Answer: B

NEW QUESTION 107
- (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 108
- (Exam Topic 15)
Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

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

Answer: A

NEW QUESTION 111
- (Exam Topic 15)
When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

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

Answer: B

NEW QUESTION 113
- (Exam Topic 15)
Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

A. Directory
B. User database
C. Multi-factor authentication (MFA)
D. Single sign-on (SSO)

Answer: A

NEW QUESTION 117
- (Exam Topic 15)
What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

A. Configuration management (CM)

B. Information Rights Management (IRM)
C. Policy creation
D. Data classification

Answer: D

NEW QUESTION 120
- (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 121
- (Exam Topic 15)
Which of the following is the MOST important rule for digital investigations?

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

Answer: C

NEW QUESTION 122
- (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 126
- (Exam Topic 15)
Which of the following is the MOST common cause of system or security failures?

A. Lack of system documentation
B. Lack of physical security controls
C. Lack of change control
D. Lack of logging and monitoring

Answer: D

NEW QUESTION 131
- (Exam Topic 15)
Which of the following is MOST important to follow when developing information security controls for an organization?

A. Exercise due diligence with regard to all risk management information to tailor appropriate controls.
B. Perform a risk assessment and choose a standard that addresses existing gaps.
C. Use industry standard best practices for security controls in the organization.
D. Review all local and international standards and choose the most stringent based on location.

Answer: C

NEW QUESTION 136
- (Exam Topic 15)
The Chief Executive Officer (CEO) wants to implement an internal audit of the company's information security posture. The CEO wants to avoid any bias in the audit process; therefore, has assigned the Sales Director to conduct the audit. After significant interaction over a period of weeks the audit concludes that the company's policies and procedures are sufficient, robust and well established. The CEO then moves on to engage an external penetration testing company in order to showcase the organization's robust information security stance. This exercise reveals significant failings in several critical security controls and shows that the incident response processes remain undocumented. What is the MOST likely reason for this disparity in the results of the audit and the external penetration test?

A. The external penetration testing company used custom zero-day attacks that could not have been predicted.
B. The information technology (IT) and governance teams have failed to disclose relevant information to the internal audit team leading to an incomplete assessment being formulated.
C. The scope of the penetration test exercise and the internal audit were significantly different.
D. The audit team lacked the technical experience and training to make insightful and objective assessments of the data provided to them.

Answer: C

NEW QUESTION 138
- (Exam Topic 15)
An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

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

Answer: A

NEW QUESTION 143
- (Exam Topic 15)
In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below.
Which of the following would be a reasonable annual loss expectation?

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

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

Answer: B

NEW QUESTION 146
- (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 151
- (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 153
- (Exam Topic 15)
A client server infrastructure that provides user-to-server authentication describes which one of the following?

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

Answer: B

NEW QUESTION 156
- (Exam Topic 15)
An application is used for funds transfer between an organization and a third-party. During a security audit, an issue with the business continuity/disaster recovery policy and procedures for this application. Which of the following reports should the audit file with the organization?

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

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

Answer: C

NEW QUESTION 157
- (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 158
- (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 161
- (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 166
- (Exam Topic 15)
A software development company has a short timeline in which to deliver a software product. The software development team decides to use open-source software libraries to reduce the development time. What concept should software developers consider when using open-source software libraries?

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

Answer: A

NEW QUESTION 167
- (Exam Topic 15)
Which of the following criteria ensures information is protected relative to its importance to the organization?

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

Answer: D

NEW QUESTION 171
- (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 173
- (Exam Topic 15)
Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

A. For the establishment, exercise, or defense of legal claims
B. The personal data has been lawfully processed and collected
C. The personal data remains necessary to the purpose for which it was collected
D. For the reasons of private interest

Answer: C

NEW QUESTION 178
- (Exam Topic 15)
A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

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

Answer: A

NEW QUESTION 180
- (Exam Topic 15)

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

Answer: D

NEW QUESTION 184
- (Exam Topic 15)
An information technology (IT) employee who travels frequently to various ies remotely to an organization' the following solutions BEST serves as a secure control mechanism to meet the organization's requirements? to troubleshoot p Which of the following solutions BEST serves as a secure control mechanisn to meet the organization's requirements?

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

Answer: D

NEW QUESTION 188
- (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 189
- (Exam Topic 15)
Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

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

Answer: B

NEW QUESTION 193
- (Exam Topic 15)
Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

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

Answer: B

NEW QUESTION 198
- (Exam Topic 15)
Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

A. Cutover
B. Walkthrough
C. Tabletop
D. Parallel

Answer: C

NEW QUESTION 203
- (Exam Topic 15)
If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), which of the following becomes even MORE essential to the assurance of network?

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

Answer: C

NEW QUESTION 204
- (Exam Topic 15)
Which of the following terms BEST describes a system which allows a user to log in and access multiple related servers and applications?

A. Remote Desktop Protocol (RDP)
B. Federated identity management (FIM)
C. Single sign-on (SSO)
D. Multi-factor authentication (MFA)

Answer: B

NEW QUESTION 208
- (Exam Topic 15)
What is the MINIMUM standard for testing a disaster recovery plan (DRP)?

A. Semi-annually and in alignment with a fiscal half-year business cycle
B. Annually or less frequently depending upon audit department requirements
C. Quarterly or more frequently depending upon the advice of the information security manager
D. As often as necessary depending upon the stability of the environment and business requirements

Answer: D

NEW QUESTION 212
- (Exam Topic 15)
Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

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

Answer: C

NEW QUESTION 217
- (Exam Topic 15)
When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

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

Answer: C

NEW QUESTION 219
- (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 223
- (Exam Topic 15)
An organization has discovered that organizational data is posted by employees to data storage accessible to the general public. What is the PRIMARY step an organization must take
to ensure data is properly protected from public release?

A. Implement a data classification policy.
B. Implement a data encryption policy.
C. Implement a user training policy.
D. Implement a user reporting policy.

Answer: C

NEW QUESTION 224
- (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 228
- (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 229
- (Exam Topic 15)
The personal laptop of an organization executive is stolen from the office, complete with personnel and project records. Which of the following should be done FIRST to mitigate future occurrences?

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

Answer: A

NEW QUESTION 230
- (Exam Topic 15)
Which of the following is the MOST significant key management problem due to the number of keys created?

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

Answer: B

NEW QUESTION 234
- (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 237
- (Exam Topic 15)
Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the

security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management's directive?

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

Answer: B

NEW QUESTION 241
- (Exam Topic 15)
What is static analysis intended to do when analyzing an executable file?

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

Answer: D

NEW QUESTION 245
- (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 248
- (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 253
- (Exam Topic 15)
What is the benefit of using Network Admission Control (NAC)?

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

Answer: C

NEW QUESTION 258
- (Exam Topic 15)
Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

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

Answer: C

NEW QUESTION 260
- (Exam Topic 15)
Which of the following is the PRIMARY issue when analyzing detailed log information?

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

Answer: D

NEW QUESTION 261
- (Exam Topic 15)
Which of the following outsourcing agreement provisions has the HIGHEST priority from a security operations perspective?

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

Answer: D

NEW QUESTION 263
- (Exam Topic 15)
Which of the following addresses requirements of security assessments during software acquisition?

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

Answer: A

NEW QUESTION 266
- (Exam Topic 15)
A Chief Information Security Officer (CISO) of a firm which decided to migrate to cloud has been tasked with ensuring an optimal level of security. Which of the following would be the FIRST consideration?

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

Answer: A

NEW QUESTION 271
- (Exam Topic 15)
Which of the following will an organization's network vulnerability testing process BEST enhance?

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

Answer: C

NEW QUESTION 275
- (Exam Topic 15)
Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

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

Answer: A

NEW QUESTION 278
- (Exam Topic 15)
Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

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

Answer: D

NEW QUESTION 280
- (Exam Topic 15)
An organization has implemented a protection strategy to secure the network from unauthorized external access. The new Chief Information Security Officer (CISO) wants to increase security by better protecting the network from unauthorized internal access. Which Network Access Control (NAC) capability BEST meets this objective?

A. Application firewall

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

Answer: D

NEW QUESTION 284
- (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 286
- (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 291
- (Exam Topic 15)
A Distributed Denial of Service (DDoS) attack was carried out using malware called Mirai to create a large-scale command and control system to launch a botnet. Which of the following devices were the PRIMARY sources used to generate the attack traffic?

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

Answer: A

NEW QUESTION 296
- (Exam Topic 15)
An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

A. Default the user to not share any information.
B. Inform the user of the sharing feature changes after implemented.
C. Share only what the organization decides is best.
D. Stop sharing data with the other users.

Answer: D

NEW QUESTION 301
- (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 306
- (Exam Topic 15)
Which of the following is required to verify the authenticity of a digitally signed document?

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

Answer: A

NEW QUESTION 307
- (Exam Topic 15)
What documentation is produced FIRST when performing an effective physical loss control process?

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

Answer: C

NEW QUESTION 312
- (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 313
- (Exam Topic 15)
Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

A. Use Media Gateway Control Protocol (MGCP)
B. Use Transport Layer Security (TLS) protocol
C. Use File Transfer Protocol (FTP)
D. Use Secure Shell (SSH) protocol

Answer: B

NEW QUESTION 315
- (Exam Topic 15)
When conducting a third-party risk assessment of a new supplier, which of the following reports should be reviewed to confirm the operating effectiveness of the security, availability, confidentiality, and privacy trust principles?

A. Service Organization Control (SOC) 1, Type 2
B. Service Organization Control (SOC) 2, Type 2
C. International Organization for Standardization (ISO) 27001
D. International Organization for Standardization (ISO) 27002

Answer: B

NEW QUESTION 318
- (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 321
- (Exam Topic 15)
The ability to send malicious code, generally in the form of a client side script, to a different end user is categorized as which type of vulnerability?

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

Answer: C

NEW QUESTION 324
- (Exam Topic 15)
Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

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

Answer: C

NEW QUESTION 326
- (Exam Topic 15)
Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

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

Answer: D

NEW QUESTION 328
- (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 333
- (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 336
- (Exam Topic 15)
An organization's internal audit team performed a security audit on the company's system and reported that the manufacturing application is rarely updated along with other issues categorized as minor. Six months later, an external audit team reviewed the same system with the same scope, but identified severe weaknesses in the manufacturing application's security controls. What is MOST likely to be the root cause of the internal audit team's failure in detecting these security issues?

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

Answer: A

NEW QUESTION 340
- (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 341
- (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 344
- (Exam Topic 15)
What Is a risk of using commercial off-the-shelf (COTS) products?

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

Answer: A

NEW QUESTION 345
- (Exam Topic 15)
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

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

Answer: A

NEW QUESTION 346
- (Exam Topic 15)
Which of the following BEST describes the purpose of software forensics?

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

Answer: D

NEW QUESTION 349
- (Exam Topic 15)
A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

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

Answer: B

NEW QUESTION 350
- (Exam Topic 15)
Which of the following types of hosts should be operating in the demilitarized zone (DMZ)?

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

Answer: A

NEW QUESTION 354
- (Exam Topic 15)
An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.
Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

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

Answer: B

NEW QUESTION 358
- (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 359
- (Exam Topic 15)
Which of the following BEST obtains an objective audit of security controls?

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

Answer: A

NEW QUESTION 363
- (Exam Topic 15)
The security team has been tasked with performing an interface test against a frontend external facing application and needs to verify that all input fields protect against
invalid input. Which of the following BEST assists this process?

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

Answer: A

NEW QUESTION 366
- (Exam Topic 15)
Which of the following is a unique feature of attribute-based access control (ABAC)?

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

Answer: C

NEW QUESTION 368
- (Exam Topic 15)
Which of the (ISC)? Code of Ethics canons is MOST reflected when preserving the value of systems, applications, and entrusted information while avoiding conflicts of interest?

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

Answer: B

NEW QUESTION 370
- (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 372
- (Exam Topic 15)
What is the FIRST step in risk management?

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

Answer: C

NEW QUESTION 373
- (Exam Topic 15)
A subscription service which provides power, climate control, raised flooring, and telephone wiring but NOT the computer and peripheral equipment is BEST described as a:

A. warm site.
B. reciprocal site.
C. sicold site.

D. hot site.

Answer: C

NEW QUESTION 377
- (Exam Topic 15)
Which of the following is a correct feature of a virtual local area network (VLAN)?

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

Answer: A

NEW QUESTION 378
- (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 382
- (Exam Topic 15)
Which of the following factors is á PRIMARY reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy?

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

Answer: B

NEW QUESTION 386
- (Exam Topic 15)
Which of the following is TRUE for an organization that is using a third-party federated identity service?

A. The organization enforces the rules to other organization's user provisioning
B. The organization establishes a trust relationship with the other organizations
C. The organization defines internal standard for overall user identification
D. The organization specifies alone how to authenticate other organization's users

Answer: C

NEW QUESTION 390
- (Exam Topic 15)
Which of the following is the MOST appropriate technique for destroying magnetic platter style hard disk drives (HDD) containing data with a "HIGH" security categorization?

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

Answer: D

NEW QUESTION 394
- (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 396
- (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 399
- (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 404
- (Exam Topic 15)
An organization is implementing data encryption using symmetric ciphers and the Chief Information Officer (CIO) is concerned about the risk of using one key to protect all sensitive data, The security practitioner has been tasked with recommending a solution to address the CIO's concerns, Which of the following is the BEST approach to achieving the objective by encrypting all sensitive data?

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

Answer: D

NEW QUESTION 409
- (Exam Topic 15)
A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?

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

Answer: D

NEW QUESTION 412
- (Exam Topic 15)
When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of big data?

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

Answer: C

NEW QUESTION 416
- (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 418
- (Exam Topic 15)
What does the result of Cost-Benefit Analysis (C8A) on new security initiatives provide?

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

Answer: A

NEW QUESTION 421
- (Exam Topic 15)
Which is the PRIMARY mechanism for providing the workforce with the information needed to protect an agency's vital information resources?

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

Answer: A

NEW QUESTION 422
- (Exam Topic 15)
Which of the following statements is TRUE about Secure Shell (SSH)?

A. SSH does not protect against man-in-the-middle (MITM) attacks.
B. SSH supports port forwarding, which can be used to protect less secured protocols.
C. SSH can be used with almost any application because it is concerned with maintaining a circuit.
D. SSH is easy to deploy because it requires a Web browser only.

Answer: B

NEW QUESTION 424
- (Exam Topic 15)
How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?

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

Answer: C

NEW QUESTION 429
- (Exam Topic 15)
What is the FIRST step in developing a patch management plan?

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

Answer: B

NEW QUESTION 434
- (Exam Topic 15)
In Identity Management (IdM), when is the verification stage performed?

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

Answer: A

NEW QUESTION 439
- (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 441
- (Exam Topic 15)
When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

A. Requirements

B. Risk assessment
C. Due diligence
D. Planning

Answer: B

NEW QUESTION 444
- (Exam Topic 15)
Digital non-repudiation requires which of the following?

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

Answer: A

NEW QUESTION 447
- (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 452
- (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 457
- (Exam Topic 15)
Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

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

Answer: A

NEW QUESTION 460
- (Exam Topic 15)
A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS).
Which of the following factors leads the company to choose an IDaaS as their solution?

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

Answer: B

NEW QUESTION 465
- (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 467

- (Exam Topic 15)
Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

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

Answer: A

NEW QUESTION 471
- (Exam Topic 15)
The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

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

Answer: D

NEW QUESTION 475
- (Exam Topic 15)
A web-based application known to be susceptible to attacks is now under review by a senior developer. The organization would like to ensure this application Is less susceptible to injection attacks specifically,
What strategy will work BEST for the organization's situation?

A. Do not store sensitive unencrypted data on the back end.
B. Whitelist input and encode or escape output before it is processed for rendering.
C. Limit privileged access or hard-coding logon credentials,
D. Store sensitive data in a buffer that retains data in operating system (OS) cache or memory.

Answer: B

NEW QUESTION 477
- (Exam Topic 15)
Which of the following BEST describes the purpose of Border Gateway Protocol (BGP)?

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

Answer: B

NEW QUESTION 478
- (Exam Topic 15)
A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

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

Answer: D

NEW QUESTION 482
- (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 483
- (Exam Topic 15)
An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 1
B. 2
C. 3

Answer: A

NEW QUESTION 487
- (Exam Topic 15)
What is the MOST common security risk of a mobile device?

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

Answer: C

NEW QUESTION 489
- (Exam Topic 15)
An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weal

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

Answer: A

NEW QUESTION 491
- (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 493
- (Exam Topic 15)
What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

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

Answer: C

NEW QUESTION 496
- (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 497
- (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 501
- (Exam Topic 15)
Why would a system be structured to isolate different classes of information from one another and segregate them by user jurisdiction?

A. The organization can avoid e-discovery processes in the event of litigation.

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

Answer: C

NEW QUESTION 504
- (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 506
- (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 507
- (Exam Topic 15)
If traveling abroad and a customs official demands to examine a personal computer, which of the following should be assumed?

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

Answer: C

NEW QUESTION 512
- (Exam Topic 15)
In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

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

Answer: A

NEW QUESTION 516
- (Exam Topic 15)
A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory risk to the company. The manager MOST likely discovered this during which of the following?

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

Answer: B

NEW QUESTION 517
- (Exam Topic 15)
Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

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

Answer: C

NEW QUESTION 521
- (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 525
- (Exam Topic 15)
Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

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

Answer: B

NEW QUESTION 526
- (Exam Topic 15)
Which type of access control includes a system that allows only users that are type=managers and department=sales to access employee records?

A. Discretionary access control (DAC)
B. Mandatory access control (MAC)
C. Role-based access control (RBAC)
D. Attribute-based access control (ABAC)

Answer: C

NEW QUESTION 530
- (Exam Topic 15)
A security engineer is assigned to work with the patch and vulnerability management group. The deployment of a new patch has been approved and needs to be applied.
The research is complete, and the security engineer has provided recommendations. Where should the patch be applied FIRST?

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

Answer: C

NEW QUESTION 535
- (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 537
- (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 541
- (Exam Topic 15)
Why are packet filtering routers used in low-risk environments?

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

Answer: B

NEW QUESTION 545
- (Exam Topic 15)
Which of the following is the name of an individual or group that is impacted by a change?

A. Change agent
B. Stakeholder
C. Sponsor
D. End User

Answer: B

NEW QUESTION 548
- (Exam Topic 15)
Which of the following BEST describes the use of network architecture in reducing corporate risks associated with mobile devices?

A. Maintaining a "closed applications model on all mobile devices depends on demilitarized 2one (DM2) servers
B. Split tunneling enabled for mobile devices improves demilitarized zone (DMZ) security posture
C. Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices
D. Applications that manage mobile devices are located in an Internet demilitarized zone (DMZ)

Answer: C

NEW QUESTION 552
- (Exam Topic 15)
A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging generates extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

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

Answer: D

NEW QUESTION 556
- (Exam Topic 15)
What is the MAIN purpose of a security assessment plan?

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

Answer: B

NEW QUESTION 560
- (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 561
- (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 563
- (Exam Topic 15)
In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

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

Answer: D

NEW QUESTION 565
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a
particular system over a 12-month period. Which type of SOC report should be utilized?

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

Answer: C

NEW QUESTION 567
- (Exam Topic 15)
Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages?

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

Answer: C

NEW QUESTION 572
- (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 573
- (Exam Topic 15)
A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

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

Answer: C

NEW QUESTION 577
- (Exam Topic 15)
An organization wants to migrate to Session Initiation Protocol (SIP) to save on telephony expenses. Which of the following security related statements should be considered in the decision-making process?

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

Answer: C

NEW QUESTION 582
- (Exam Topic 15)
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

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

Answer: A

NEW QUESTION 586
- (Exam Topic 15)
Which of the following VPN configurations should be used to separate Internet and corporate traffic?

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

Answer: A

NEW QUESTION 591
- (Exam Topic 15)
A security professional is assessing the risk in an application and does not take into account any mitigating or compensating controls. This type of risk rating is an example of which of the following?

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

Answer: B

NEW QUESTION 592
- (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 595
- (Exam Topic 15)
Which media sanitization methods should be used for data with a high security categorization?

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

Answer: D

NEW QUESTION 596
- (Exam Topic 15)
How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

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

Answer: C

NEW QUESTION 600
- (Exam Topic 15)
Which of the following roles is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications?

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

Answer: D

NEW QUESTION 603
- (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 605
- (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 609
- (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 610
- (Exam Topic 15)
An organization is considering partnering with a third-party supplier of cloud services. The organization will only be providing the data and the third-party supplier will be providing the security controls. Which of the following BEST describes this service offering?

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

Answer: D

NEW QUESTION 611
- (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 612
- (Exam Topic 15)
The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in which role in order to ensure proper protection of data during and after the cloud migration?

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

Answer: A

NEW QUESTION 617
- (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 619
- (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 620
- (Exam Topic 15)
What is the MOST common cause of Remote Desktop Protocol (RDP) compromise?

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

Answer: B

NEW QUESTION 621
- (Exam Topic 15)
Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

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

Answer: C

NEW QUESTION 622
- (Exam Topic 15)
An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a
per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

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

Answer: A

NEW QUESTION 626
- (Exam Topic 15)
Which of the following is a canon of the (ISC)2 Code of Ethics?

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

Answer: C

NEW QUESTION 631
- (Exam Topic 15)
What is the MOST appropriate hierarchy of documents when implementing a security program?

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

Answer: C

NEW QUESTION 634
- (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 636
- (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 638
- (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 643
- (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 648
- (Exam Topic 15)
Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

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

Answer: D

NEW QUESTION 653
- (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 655
- (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 660
- (Exam Topic 15)
Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device which has been stolen?

A. Mobile Device Management (MDM) with device wipe
B. Whole device encryption with key escrow
C. Virtual private network (VPN) with traffic encryption
D. Mobile device tracking with geolocation

Answer: A

NEW QUESTION 661
- (Exam Topic 15)
What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

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

Answer: C

NEW QUESTION 663
- (Exam Topic 15)
Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

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

Answer: A

NEW QUESTION 665
- (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 667
- (Exam Topic 15)
A large organization's human resources and security teams are planning on implementing technology to eliminate manual user access reviews and improve compliance. Which of the following options is MOST likely to resolve the issues associated with user access?

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

Answer: B

NEW QUESTION 668
- (Exam Topic 15)
Building blocks for software-defined networks (SDN) require which of the following?

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

Answer: C

NEW QUESTION 669
- (Exam Topic 14)
What form of attack could this represent?

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

Answer: D

NEW QUESTION 670
- (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 672
- (Exam Topic 14)
Which of the following media is LEAST problematic with data remanence?

A. Dynamic Random Access Memory (DRAM)
B. Electrically Erasable Programming Read-Only Memory (BPRCM)
C. Flash memory
D. Magnetic disk

Answer: A

NEW QUESTION 673
- (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 678
- (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 683
- (Exam Topic 14)
What should an auditor do when conducting a periodic audit on media retention?

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

Answer: A

NEW QUESTION 684
- (Exam Topic 14)
What is a warn site when conducting Business continuity planning (BCP)

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

Answer: B

NEW QUESTION 688
- (Exam Topic 14)
Which of the following is used to support the concept of defense in depth during the development phase of a software product?

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

Answer: B

NEW QUESTION 690
- (Exam Topic 14)
copyright provides protection for which of the following?

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

Answer: C

NEW QUESTION 691
- (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 696
- (Exam Topic 14)
How long should the records on a project be retained?

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

Answer: B

NEW QUESTION 698
- (Exam Topic 14)
What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

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

Answer: D

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

NEW QUESTION 701
- (Exam Topic 14)
A large corporation is looking for a solution to automate access based on where the request is coming from, who the user is, what device they are connecting with, and what and time of day they are attempting this access. What type of solution would suit their needs?

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

Answer: B

NEW QUESTION 703
- (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 705
- (Exam Topic 14)
Which of the following encryption types is used in Hash Message Authentication Code (HMAC) for key distribution?

A. Symmetric
B. Asymmetric
C. Ephemeral
D. Permanent

Answer: A

Explanation:
Reference: https://www.brainscape.com/flashcards/cryptography-message-integrity-6886698/packs/10957693

NEW QUESTION 710
- (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 714
- (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 717
- (Exam Topic 14)
Additional padding may be added to toe Encapsulating Security Protocol (ESP) b trailer to provide which of the following?

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

Answer: C

NEW QUESTION 718
- (Exam Topic 14)
What are the roles within a scrum methodology?

A. Scrum master, retirements manager, and development team
B. System owner, scrum master, and development team
C. Scrum master, quality assurance team, and scrum team
D. Product owner, scrum master, and scrum team

Answer: D

NEW QUESTION 723
- (Exam Topic 14)
Which of the following is mobile device remote fingerprinting?

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

Answer: C

NEW QUESTION 727
- (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 728
- (Exam Topic 14)
How can an attacker exploit overflow to execute arbitrary code?

A. Modify a function's return address.

B. Alter the address of the stack.
C. Substitute elements in the stack.
D. Move the stack pointer.

Answer: A

NEW QUESTION 731
- (Exam Topic 14)
Which of the following is a characteristic of convert security testing?

A. Induces less risk than over testing
B. Tests staff knowledge and Implementation of the organization's security policy
C. Focuses an Identifying vulnerabilities
D. Tests and validates all security controls in the organization

Answer: B

NEW QUESTION 733
- (Exam Topic 14)
Which of the following is a method of attacking internet (IP) v6 Layer 3 and Layer 4 ?

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

Answer: A

NEW QUESTION 734
- (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 736
- (Exam Topic 14)
Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

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

Answer: A

Explanation:
Reference: https://portswigger.net/web-security/csrf

NEW QUESTION 741
- (Exam Topic 14)
A criminal organization is planning an attack on a government network. Which of the following is the MOST severe attack to the network availability?

A. Network management communications is disrupted by attacker
B. Operator loses control of network devices to attacker
C. Sensitive information is gathered on the network topology by attacker
D. Network is flooded with communication traffic by attacker

Answer: B

NEW QUESTION 746
- (Exam Topic 14)
During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should en assessor do?

A. Increase the number and type of relevant staff to interview.
B. Conduct a comprehensive examination of the Disaster Recovery Plan (DRP).
C. Increase the level of detail of the interview questions.
D. Conduct a detailed review of the organization's DR policy.

Answer: A

NEW QUESTION 750
- (Exam Topic 14)
When selecting a disk encryption technology, which of the following MUST also be assured to be encrypted?

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

Answer: A

NEW QUESTION 752
- (Exam Topic 14)
Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

A. Data Loss Protection (DIP), firewalls, data classification
B. Least privilege access, Data Loss Protection (DLP), physical access controls
C. Staff vetting, least privilege access, Data Loss Protection (DLP)
D. Background checks, data encryption, web proxies

Answer: B

NEW QUESTION 755
- (Exam Topic 14)
Which of the following is the MOST critical success factor in the security patch management process?

A. Tracking and reporting on inventory
B. Supporting documentation
C. Management review of reports
D. Risk and impact analysis

Answer: A

NEW QUESTION 759
- (Exam Topic 14)
What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

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

Answer: B

NEW QUESTION 762
- (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 764
- (Exam Topic 14)
In order for application developers to detect potential vulnerabilities earlier during the Software Development Life Cycle (SDLC), which of the following safeguards should be implemented FIRST as part of a comprehensive testing framework?

A. Source code review
B. Acceptance testing
C. Threat modeling
D. Automated testing

Answer: A

NEW QUESTION 765
- (Exam Topic 14)
Which of the following BEST provides for non-repudiation od user account actions?

A. Centralized authentication system
B. File auditing system
C. Managed Intrusion Detection System (IDS)
D. Centralized logging system

Answer: D

NEW QUESTION 767
- (Exam Topic 14)
Which of the following controls is the most for a system identified as critical in terms of data and function to the organization?

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

Answer: B

NEW QUESTION 772
- (Exam Topic 14)
The core component of Role Based Access control (RBAC) must be constructed of defined data elements. Which elements are required?

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

Answer: B

NEW QUESTION 775
- (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 776
- (Exam Topic 14)
Which of the following is the BEST statement for a professional to include as port of business continuity (BC) procedure?

A. A full data backup must be done upon management request.
B. An incremental data backup must be done upon management request.
C. A full data backup must be done based on the needs of the business.
D. In incremental data backup must be done after each system change.

Answer: D

NEW QUESTION 778
- (Exam Topic 14)
When a flaw in Industrial control (ICS) software is discovered, what is the GREATEST impediment to deploying a patch?

A. Many IG systems have software that is no longer being maintained by the venders.
B. Compensating controls may impact IG performance.
C. Testing a patch in an IG may require more resources than the organization can commit.
D. vendors are required to validate the operability patches.

Answer: D

NEW QUESTION 783
- (Exam Topic 14)
What is the PRIMARY benefit of analyzing the partition layout of a hard disk volume when performing forensic analysis?

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

Answer: A

NEW QUESTION 786
- (Exam Topic 14)
Which open standard could l large corporation deploy for authorization services for single sign-on (SSO) use across multiple internal and external application?

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

Answer: B

NEW QUESTION 790
- (Exam Topic 14)
Which of the following BEST describes how access to a system is granted to federated user accounts?

A. With the federation assurance level
B. Based on defined criteria by the Relying Party (RP)
C. Based on defined criteria by the Identity Provider (IdP)
D. With the identity assurance level

Answer: C

Explanation:
Reference: https://resources.infosecinstitute.com/cissp-domain-5-refresh-identity-and-access-management/

NEW QUESTION 792
- (Exam Topic 14)
Which of the following is the MOST important activity an organization performs to ensure that securiy is part of the overall organization culture?

A. Ensue security policies are issued to all employees
B. Perform formal reviews of security Incidents.
C. Manage a program of security audits.
D. Work with senior management to meet business goals.

Answer: C

NEW QUESTION 794
- (Exam Topic 14)
Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

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

Answer: C

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

NEW QUESTION 798
- (Exam Topic 14)
Which of the following needs to be included in order for High Availability (HA) to continue operations during planned system outages?

A. Redundant hardware, disk spanning, and patching
B. Load balancing, power reserves, and disk spanning
C. Backups, clustering, and power reserves
D. Clustering, load balancing, and fault-tolerant options

Answer: D

NEW QUESTION 800
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

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

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