Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

NEW QUESTION 1
- (Exam Topic 15)
What is the FIRST step when developing an Information Security Continuous Monitoring (ISCM) program?

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

Answer: D

NEW QUESTION 2
- (Exam Topic 15)
In addition to life, protection of which of the following elements is MOST important when planning a data center site?

A. Data and hardware
B. Property and operations
C. Profits and assets
D. Resources and reputation

Answer: D

NEW QUESTION 3
- (Exam Topic 15)
An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration test is needed?

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

Answer: C

NEW QUESTION 4
- (Exam Topic 15)
In which process MUST security be considered during the acquisition of new software?

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

Answer: B

NEW QUESTION 5
- (Exam Topic 15)
Which of the following is the top barrier for companies to adopt cloud technology?

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

Answer: D

NEW QUESTION 6
- (Exam Topic 15)
Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

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

Answer: B

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 15)
Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-systems gracefully handle invalid input?

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

Answer: B

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

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

Answer: B

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

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

Answer: B

NEW QUESTION 11
- (Exam Topic 15)
Which of the following is fundamentally required to address potential security issues when initiating software development?

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

Answer: C

NEW QUESTION 15
- (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 19
- (Exam Topic 15)
Which of the following is a PRIMARY security weakness in the design of Domain Name System (DNS)?

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

Answer: A

NEW QUESTION 20
- (Exam Topic 15)
Which of the following provides the MOST secure method for Network Access Control (NAC)?

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

Answer: B

NEW QUESTION 24
- (Exam Topic 15)
Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

A. Check the technical design.
B. Conduct a site survey.
C. Categorize assets.
D. Choose a suitable location.

Answer: A

NEW QUESTION 27
- (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 29
- (Exam Topic 15)
An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP), The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract.
Which of the following MUST be included in the contract?

A. A detailed overview of all equipment involved in the outsourcing contract
B. The MSSP having an executive manager responsible for information security
C. The right to perform security compliance tests on the MSSP's equipment
D. The right to audit the MSSP's security process

Answer: C

NEW QUESTION 32
- (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 37
- (Exam Topic 15)
Which of the following is the strongest physical access control?

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

Answer: D

NEW QUESTION 39
- (Exam Topic 15)
What type of database attack would allow a customer service employee to determine quarterly sales results before they are publically announced?

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

Answer: A

NEW QUESTION 44
- (Exam Topic 15)
A company is moving from the V model to Agile development. How can the information security department BEST ensure that secure design principles are implemented in the new methodology?

A. All developers receive a mandatory targeted information security training.
B. The non-financial information security requirements remain mandatory for the new model.
C. The information security department performs an information security assessment after each sprint.
D. Information security requirements are captured in mandatory user stories.

Answer: D

NEW QUESTION 45
- (Exam Topic 15)
Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

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

Answer: A

NEW QUESTION 46
- (Exam Topic 15)
Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

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

Answer: B

NEW QUESTION 47
- (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 49
- (Exam Topic 15)
Recently, an unknown event has disrupted a single Layer-2 network that spans between two geographically diverse data centers. The network engineers have asked for assistance in identifying the root cause of the event. Which of the following is the MOST likely cause?

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

Answer: D

NEW QUESTION 50
- (Exam Topic 15)
A security practitioner has been asked to model best practices for disaster recovery (DR) and business continuity. The practitioner has decided that a formal committee is needed to establish a business continuity policy. Which of the following BEST describes this stage of business continuity development?

A. Project Initiation and Management
B. Risk Evaluation and Control

C. Developing and Implementing business continuity plans (BCP)
D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 51
- (Exam Topic 15)
What is the P R IM A R Y reason criminal law is difficult to enforce when dealing with cyber-crime?

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

Answer: D

NEW QUESTION 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 58
- (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 63
- (Exam Topic 15)
A software developer installs a game on their organization-provided smartphone. Upon installing the game, the software developer is prompted to allow the game access to call logs, Short Message Service (SMS) messaging, and Global Positioning System (GPS) location data. What has the game MOST likely introduced to the smartphone?

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

Answer: B

NEW QUESTION 66
- (Exam Topic 15)
In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

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

Answer: B

NEW QUESTION 68
- (Exam Topic 15)
Why is authentication by ownership stronger than authentication by knowledge?

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

Answer: B

NEW QUESTION 69

- (Exam Topic 15)
A project manager for a large software firm has acquired a government contract that generates large amounts of Controlled Unclassified Information (CUI). The organization's information security manager has received a request to transfer project-related CUI between systems of differing security classifications. What role provides
the authoritative guidance for this transfer?

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

Answer: C

NEW QUESTION 73
- (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 75
- (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 78
- (Exam Topic 15)
Which of the following is the BEST way to mitigate circumvention of access controls?

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

Answer: D

NEW QUESTION 83
- (Exam Topic 15)
Which of the following is an indicator that a company's new user security awareness training module has been effective?

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

Answer: B

NEW QUESTION 86
- (Exam Topic 15)
Which of the following implementations will achieve high availability in a website?

A. Multiple Domain Name System (DNS) entries resolving to the same web server and large amounts of bandwidth
B. Disk mirroring of the web server with redundant disk drives in a hardened data center
C. Disk striping of the web server hard drives and large amounts of bandwidth
D. Multiple geographically dispersed web servers that are configured for failover

Answer: D

NEW QUESTION 88
- (Exam Topic 15)
Which of the following examples is BEST to minimize the attack surface for a customer's private information?

A. Obfuscation
B. Collection limitation
C. Authentication
D. Data masking

Answer: A

NEW QUESTION 91
- (Exam Topic 15)
A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

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

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

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

Answer: A

NEW QUESTION 92
- (Exam Topic 15)
Who should formulate conclusions from a particular digital fore Ball, Submit a Toper Of Tags, and the results?

A. The information security professional's supervisor
B. Legal counsel for the information security professional's employer
C. The information security professional who conducted the analysis
D. A peer reviewer of the information security professional

Answer: B

NEW QUESTION 97
- (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 98
- (Exam Topic 15)
Physical Access Control Systems (PACS) allow authorized security personnel to manage and monitor access control for subjects through which function?

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

Answer: B

NEW QUESTION 100
- (Exam Topic 15)
A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

A. Availability
B. Disaster recovery (DR)
C. Redundancy
D. Business continuity (BC)

Answer: D

NEW QUESTION 101
- (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 106
- (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 109
- (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 110
- (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 111
- (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 115
- (Exam Topic 15)
Which of the following are mandatory canons for the (ISC)* Code of Ethics?

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

Answer: D

NEW QUESTION 119
- (Exam Topic 15)
Which of the following addresses requirements of security assessment during software acquisition?

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

Answer: B

NEW QUESTION 124
- (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 125
- (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 129
- (Exam Topic 15)
In which of the following system life cycle processes should security requirements be developed?

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

Answer: B

NEW QUESTION 132
- (Exam Topic 15)
Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management
decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

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

Answer: A

NEW QUESTION 137
- (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 142
- (Exam Topic 15)
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

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

Answer: C

NEW QUESTION 146
- (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 148
- (Exam Topic 15)
A security professional should ensure that clients support which secondary algorithm for digital signatures when a Secure Multipurpose Internet Mail Extension (S/MIME) is used?

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

Answer: C

NEW QUESTION 150
- (Exam Topic 15)
Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

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

Answer: B

NEW QUESTION 155
- (Exam Topic 15)
Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

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

Answer: D

NEW QUESTION 160
- (Exam Topic 15)
Computer forensics requires which of the following MAIN steps?

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

Answer: B

NEW QUESTION 164
- (Exam Topic 15)
The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

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

Answer: B

NEW QUESTION 166
- (Exam Topic 15)
An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

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

Answer: D

NEW QUESTION 170
- (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 173
- (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 174
- (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 177
- (Exam Topic 15)
A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

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

Answer: B

NEW QUESTION 179
- (Exam Topic 15)
Before implementing an internet-facing router, a network administrator ensures that the equipment is baselined/hardened according to approved configurations and settings. This action provides protection against which of the following attacks?

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

Answer: B

NEW QUESTION 182
- (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 186
- (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 191
- (Exam Topic 15)
Dumpster diving is a technique used in which stage of penetration testing methodology?

A. Attack
B. Discovery
C. Reporting
D. Planning

Answer: B

NEW QUESTION 196
- (Exam Topic 15)
Using Address Space Layout Randomization (ASLR) reduces the potential for which of the following attacks?

A. SQL injection (SQLi)
B. Man-in-the-middle (MITM)
C. Cross-Site Scripting (XSS)
D. Heap overflow

Answer: D

NEW QUESTION 201
- (Exam Topic 15)
When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

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

Answer: C

NEW QUESTION 206
- (Exam Topic 15)
When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network. Which of the following will BEST help secure the VoIP network?

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

Answer: A

NEW QUESTION 210
- (Exam Topic 15)
An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

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

Answer: B

NEW QUESTION 212
- (Exam Topic 15)
What is the MOST important goal of conducting security assessments?

A. To prepare the organization for an external audit, particularly by a regulatory entity
B. To discover unmitigated security vulnerabilities, and propose paths for mitigating them
C. To align the security program with organizational risk appetite
D. To demonstrate proper function of security controls and processes to senior management

Answer: B

NEW QUESTION 215
- (Exam Topic 15)
An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

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

Answer: D

NEW QUESTION 220
- (Exam Topic 15)
What is the FINAL step in the waterfall method for contingency planning?

A. Maintenance
B. Testing
C. Implementation
D. Training

Answer: A

NEW QUESTION 225
- (Exam Topic 15)
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 230
- (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 235
- (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 239
- (Exam Topic 15)
In setting expectations when reviewing the results of a security test, which of the following statements is MOST important to convey to reviewers?

A. The target's security posture cannot be further compromised.
B. The results of the tests represent a point-in-time assessment of the target(s).
C. The accuracy of testing results can be greatly improved if the target(s) are properly hardened.
D. The deficiencies identified can be corrected immediately

Answer: C

NEW QUESTION 240
- (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 244
- (Exam Topic 15)
Which of the following is MOST appropriate to collect evidence of a zero-day attack?

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

Answer: A

NEW QUESTION 248
- (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 252
- (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 255
- (Exam Topic 15)
In a large company, a system administrator needs to assign users access to files using Role Based Access Control (RBAC). Which option Is an example of RBAC?

A. Mowing users access to files based on their group membership
B. Allowing users access to files based on username
C. Allowing users access to files based on the users location at time of access
D. Allowing users access to files based on the file type

Answer: A

NEW QUESTION 258
- (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 261
- (Exam Topic 15)
An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of which of the following types of attack?

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

Answer: B

NEW QUESTION 265
- (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 268
- (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 269
- (Exam Topic 15)
What are the essential elements of a Risk Assessment Report (RAR)?

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

Answer: D

NEW QUESTION 274
- (Exam Topic 15)
When defining a set of security controls to mitigate a risk, which of the following actions MUST occur?

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

Answer: A

NEW QUESTION 276
- (Exam Topic 15)
An organization is planning to have an it audit of its as a Service (SaaS) application to demonstrate to external parties that the security controls around availability are designed. The audit report must also cover a certain period of time to show the operational effectiveness of the controls. Which Service Organization Control (SOC) report would BEST fit their needs?

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

Answer: D

NEW QUESTION 277
- (Exam Topic 15)
Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

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

Answer: B

NEW QUESTION 280
- (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 284
- (Exam Topic 15)
An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is MOST critical in creating acceptance tests or acceptance criteria for each release?

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

Answer: D

NEW QUESTION 286
- (Exam Topic 15)
Which of the following is the PRIMARY goal of logical access controls?

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

Answer: C

NEW QUESTION 291
- (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 295
- (Exam Topic 15)
A network security engineer needs to ensure that a security solution analyzes traffic for protocol manipulation and various sorts of common attacks. In addition, all Uniform Resource Locator (URL) traffic must be inspected and users prevented from browsing inappropriate websites. Which of the following solutions should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis?

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

Answer: B

NEW QUESTION 300
- (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 305
- (Exam Topic 15)
Which of the following events prompts a review of the disaster recovery plan (DRP)?

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

Answer: D

NEW QUESTION 310
- (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 315
- (Exam Topic 15)
Where can the Open Web Application Security Project (OWASP) list of associated vulnerabilities be found?

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

D. OWASP Mobile Project

Answer: A

NEW QUESTION 319
- (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 320
- (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 323
- (Exam Topic 15)
Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

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

Answer: A

NEW QUESTION 327
- (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 329
- (Exam Topic 15)
What requirement MUST be met during internal security audits to ensure that all information provided is expressed as an objective assessment without risk of retaliation?

A. The auditor must be independent and report directly to the management.
B. The auditor must utilize automated tools to back their findings.
C. The auditor must work closely with both the information Technology (IT) and security sections of an organization.
D. The auditor must perform manual reviews of systems and processes.

Answer: A

NEW QUESTION 334
- (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 341
- (Exam Topic 15)
According to the (ISC)? ethics canon “act honorably, honestly, justly, responsibly, and legally," which order should be used when resolving conflicts?

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

Answer: A

NEW QUESTION 344
- (Exam Topic 15)
An organization recently suffered from a web-application attack that resulted in stolen user session cookie information. The attacker was able to obtain the information when a user’s browser executed a script upon visiting a compromised website. What type of attack MOST likely occurred?

A. Cross-Site Scripting (XSS)
B. Extensible Markup Language (XML) external entities
C. SQL injection (SQLI)
D. Cross-Site Request Forgery (CSRF)

Answer: A

NEW QUESTION 345
- (Exam Topic 15)
The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

A. Removal of service accounts from review
B. Segregation of Duties (SoD)
C. Clear provisioning policies
D. Frequent audits

Answer: C

NEW QUESTION 350
- (Exam Topic 15)
What Is a risk of using commercial off-the-shelf (COTS) products?

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

Answer: A

NEW QUESTION 354
- (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 355
- (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 356
- (Exam Topic 15)
A software engineer uses automated tools to review application code and search for application flaws, back doors, or other malicious code. Which of the following is the FIRST Software Development Life Cycle (SDLC) phase where this takes place?

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

Answer: C

NEW QUESTION 359
- (Exam Topic 15)
If an employee transfers from one role to another, which of the following actions should this trigger within the identity and access management (IAM) lifecycle?

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

Answer: B

NEW QUESTION 361
- (Exam Topic 15)
Which of the following is the MOST common use of the Online Certificate Status Protocol (OCSP)?

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

Answer: D

NEW QUESTION 366
- (Exam Topic 15)
What is the MOST significant benefit of role-based access control (RBAC)?

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

Answer: A

NEW QUESTION 368
- (Exam Topic 15)
When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

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

Answer: C

NEW QUESTION 373
- (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 376
- (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 377
- (Exam Topic 15)
Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

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

Answer: A

NEW QUESTION 380
- (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 381
- (Exam Topic 15)
Which of the following MUST be done before a digital forensics investigator may acquire digital evidence?

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

Answer: C

NEW QUESTION 386
- (Exam Topic 15)
A new site's gateway isn't able to form a tunnel to the existing site-to-site Internet Protocol Security (IPsec) virtual private network (VPN) device at headquarters. Devices at the new site have no problem accessing resources on the Internet. When testing connectivity between the remote site’s gateway, it was observed that the external Internet Protocol (IP) address of the gateway was set to 192.168.1.1. and was configured to send outbound traffic to the Internet Service Provider (ISP) gateway at4 192.168.1.2. Which of the following would be the BEST way to resolve the issue and get the remote site connected?

A. Enable IPSec tunnel mode on the VPN devices at the new site and the corporate headquarters.
B. Enable Layer 2 Tunneling Protocol (L2TP) on the VPN devices at the new site and the corporate headquarters.
C. Enable Point-to-Point Tunneling Protocol (PPTP) on the VPN devices at the new site and the corporate headquarters.
D. Enable Network Address Translation (NAT) - Traversal on the VPN devices at the new site and the corporate headquarters.

Answer: A

NEW QUESTION 389
- (Exam Topic 15)
At what stage of the Software Development Life Cycle (SDLC) does software vulnerability remediation MOST likely cost the least to implement?

A. Development
B. Testing
C. Deployme
D. Design

Answer: D

NEW QUESTION 392
- (Exam Topic 15)
Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

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

Answer: A

NEW QUESTION 397

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

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

Answer: B

NEW QUESTION 399
- (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 404
- (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 406
- (Exam Topic 15)
Which of the following attack types can be used to compromise the integrity of data during transmission?

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

Answer: B

NEW QUESTION 408
- (Exam Topic 15)
The security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network. Which solution is MOST effective at discovering a successful network breach?

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

Answer: A

NEW QUESTION 411
- (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 412
- (Exam Topic 15)
A software development company found odd behavior in some recently developed software, creating a need for a more thorough code review. What is the MOST effective argument for a more thorough code review?

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

Answer: D

NEW QUESTION 414
- (Exam Topic 15)
Which of the following is the PRIMARY type of cryptography required to support non-repudiation of a digitally signed document?

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

Answer: A

NEW QUESTION 416
- (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 419
- (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 422
- (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 424
- (Exam Topic 15)
Which technique helps system designers consider potential security concerns of their systems and applications?

A. Penetration testing
B. Threat modeling
C. Manual inspections and reviews
D. Source code review

Answer: B

NEW QUESTION 428
- (Exam Topic 15)
An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

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

Answer: B

NEW QUESTION 430
- (Exam Topic 15)
Which of the following is a limitation of the Bell-LaPadula model?

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

Answer: A

NEW QUESTION 433
- (Exam Topic 15)
An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

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

Answer: A

NEW QUESTION 435
- (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 436
- (Exam Topic 15)
A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

A. nslookup
B. netstat -a
C. ipeonfig /a
D. arp -a

Answer: B

NEW QUESTION 441
- (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

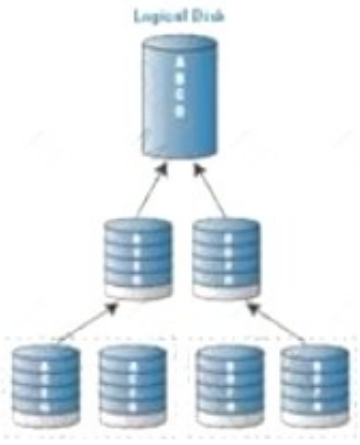
Answer: D

NEW QUESTION 443
- (Exam Topic 15)
Which of the following BEST ensures the integrity of transactions to intended recipients?

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

Answer: A

NEW QUESTION 445
- (Exam Topic 15)
Which Redundant Array c/ Independent Disks (RAID) Level does the following diagram represent?



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

Answer: D

NEW QUESTION 447
- (Exam Topic 15)
What is the PRIMARY objective of business continuity planning?

A. Establishing a cost estimate for business continuity recovery operations
B. Restoring computer systems to normal operations as soon as possible
C. Strengthening the perceived importance of business continuity planning among senior management
D. Ensuring timely recovery of mission-critical business processes

Answer: B

NEW QUESTION 451
- (Exam Topic 15)
The security architect has been assigned the responsibility of ensuring integrity of the organization's electronic records. Which of the following methods provides the strongest level of integrity?

A. Time stamping
B. Encryption
C. Hashing
D. Digital signature

Answer: D

NEW QUESTION 453
- (Exam Topic 15)
A large manufacturing organization arranges to buy an industrial machine system to produce a new line of products. The system includes software provided to the vendor by a thirdparty organization. The financial risk to the manufacturing organization starting production is high. What step should the manufacturing organization take to minimize its financial risk in the new venture prior to the purchase?

A. Hire a performance tester to execute offline tests on a system.
B. Calculate the possible loss in revenue to the organization due to software bugs and vulnerabilities, and compare that to the system's overall price.
C. Place the machine behind a Layer 3 firewall.
D. Require that the software be thoroughly tested by an accredited independent software testing company.

Answer: B

NEW QUESTION 458
- (Exam Topic 15)
What is the BEST method to use for assessing the security impact of acquired software?

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

Answer: B

NEW QUESTION 461
- (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 464
- (Exam Topic 15)
When telephones in a city are connected by a single exchange, the caller can only connect with the switchboard operator. The operator then manually connects the call.
This is an example of which type of network topology?

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

Answer: A

NEW QUESTION 467
- (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 471
- (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 474
- (Exam Topic 15)
Which of the following has the responsibility of information technology (IT) governance?

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

Answer: A

NEW QUESTION 477
- (Exam Topic 15)
International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

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

Answer: C

NEW QUESTION 478
- (Exam Topic 15)
What term is commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB)?

A. Configuration element
B. Asset register
C. Ledger item
D. Configuration item

Answer: D

NEW QUESTION 479
- (Exam Topic 15)
What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

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

Answer: D

NEW QUESTION 481
- (Exam Topic 15)
An employee's home address should be categorized according to which of the following references?

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

Answer: B

NEW QUESTION 483
- (Exam Topic 15)
When developing an organization's information security budget, it is important that the

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

Answer: A

NEW QUESTION 486
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

A. Skill set and training
B. Headcount and capacity
C. Tools and technologies
D. Scope and service catalog

Answer: C

NEW QUESTION 491
- (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 495
- (Exam Topic 15)
A hacker can use a lockout capability to start which of the following attacks?

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

Answer: A

NEW QUESTION 497
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

Answer: B

NEW QUESTION 499

- (Exam Topic 15)
In software development, developers should use which type of queries to prevent a Structured Query Language (SQL) injection?

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

Answer: A

NEW QUESTION 501
- (Exam Topic 15)
Which of the following is the MOST important consideration in selecting a security testing method based on different Radio-Frequency Identification (RFID) vulnerability types?

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

Answer: C

NEW QUESTION 505
- (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 507
- (Exam Topic 15)
A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

A. Upgrade the software affected by the vulnerability.
B. Inform management of possible risks.
C. Mitigate the risks with compensating controls.
D. Remove the affected software from the servers.

Answer: C

NEW QUESTION 512
- (Exam Topic 15)
When conducting a remote access session using Internet Protocol Security (IPSec), which Open Systems Interconnection (OSI) model layer does this connection use?

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

Answer: B

NEW QUESTION 515
- (Exam Topic 15)
Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

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

Answer: A

NEW QUESTION 519
- (Exam Topic 15)
Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

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

Answer: A

NEW QUESTION 523
- (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 528
- (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 531
- (Exam Topic 15)
A Certified Information Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to4 perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)? Code of Professional Ethics, which of the following should the CISSP do?

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

Answer: C

NEW QUESTION 534
- (Exam Topic 15)
Which of the following is the BEST method to gather evidence from a computer's hard drive?

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

Answer: D

NEW QUESTION 538
- (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 543
- (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 547
- (Exam Topic 15)
Which of the following is a security weakness in the evaluation of common criteria (CC) products?

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

Answer: A

NEW QUESTION 550
- (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 555
- (Exam Topic 15)
A security engineer is required to integrate security into a software project that is implemented by small groups test quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process'

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

Answer: C

NEW QUESTION 556
- (Exam Topic 15)
An organization with divisions in the United States (US) and the United Kingdom (UK) processes data comprised of personal information belonging to subjects living in the European Union (EU) and in the US. Which data MUST be handled according to the privacy protections of General Data Protection Regulation (GDPR)?

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

Answer: A

NEW QUESTION 561
- (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 566
- (Exam Topic 15)
Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

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

Answer: A

NEW QUESTION 568
- (Exam Topic 15)
Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

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

Answer: C

NEW QUESTION 571
- (Exam Topic 15)
A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

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

Answer: D

NEW QUESTION 575
- (Exam Topic 15)
What is the FIRST step prior to executing a test of an organisation's disaster recovery (DR) or business continuity plan (BCP)?

A. identify key stakeholders,
B. Develop recommendations for disaster scenarios.
C. Identify potential failure points.
D. Develop clear evaluation criteria.

Answer: D

NEW QUESTION 580
- (Exam Topic 15)
The application owner of a system that handles confidential data leaves an organization. It is anticipated that a replacement will be hired in approximately six months. During that time, which of the following should the organization do?

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

Answer: B

NEW QUESTION 582
- (Exam Topic 15)
A company needs to provide employee access to travel services, which are hosted by a third-party service provider, Employee experience is important, and when users are already authenticated, access to the travel portal is seamless. Which of the following methods is used to share information and grant user access to the travel portal?

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

Answer: D

NEW QUESTION 585
- (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 590
- (Exam Topic 15)
Which of the following BEST describes when an organization should conduct a black box security audit on a new software product?

A. When the organization wishes to check for non-functional compliance
B. When the organization wants to enumerate known security vulnerabilities across their infrastructure
C. When the organization has experienced a security incident
D. When the organization is confident the final source code is complete

Answer: B

NEW QUESTION 593
- (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 594
- (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 596
- (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 598
- (Exam Topic 15)
Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

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

Answer: B

NEW QUESTION 603
- (Exam Topic 15)
An information security professional is reviewing user access controls on a customer-facing application. The application must have multi-factor authentication (MFA) in place. The application currently requires a username and password to login. Which of the following options would BEST implement MFA?

A. Geolocate the user and compare to previous logins
B. Require a pre-selected number as part of the login
C. Have the user answer a secret question that is known to them
D. Enter an automatically generated number from a hardware token

Answer: C

NEW QUESTION 604
- (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 609
- (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 610
- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 613
- (Exam Topic 15)
Which of the following contributes MOST to the effectiveness of a security officer?

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

Answer: A

NEW QUESTION 616
- (Exam Topic 15)
Which of the following is an important design feature for the outer door o f a mantrap?

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

Answer: D

NEW QUESTION 619
- (Exam Topic 15)
During testing, where are the requirements to inform parent organizations, law enforcement, and a computer incident response team documented?

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

Answer: D

NEW QUESTION 622
- (Exam Topic 15)
In order to provide dual assurance in a digital signature system, the design MUST include which of the following?

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

Answer: B

NEW QUESTION 623
- (Exam Topic 15)
Which of the following activities should a forensic examiner perform FIRST when determining the priority of digital evidence collection at a crime scene?

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

Answer: C

NEW QUESTION 628
- (Exam Topic 15)
When are security requirements the LEAST expensive to implement?

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

Answer: D

NEW QUESTION 631
- (Exam Topic 15)
Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

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

Answer: C

NEW QUESTION 633
- (Exam Topic 15)
Which is MOST important when negotiating an Internet service provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over Internet Protocol (VoIP) services?

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

Answer: B

NEW QUESTION 637
- (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 642
- (Exam Topic 15)
Which of the following should exist in order to perform a security audit?

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

Answer: D

NEW QUESTION 645
- (Exam Topic 15)
What is the PRIMARY purpose of auditing, as it relates to the security review cycle?

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

Answer: A

NEW QUESTION 649
- (Exam Topic 15)
While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team?

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

Answer: C

NEW QUESTION 651
- (Exam Topic 15)
What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

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

Answer: B

NEW QUESTION 654
- (Exam Topic 15)
When recovering from an outage, what is the Recovery Point Objective (RPO), in terms of data recovery?

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

Answer: B

NEW QUESTION 658
- (Exam Topic 15)
To comply with industry requirements, a security assessment on the cloud server should identify which protocols and weaknesses are being exposed to attackers on the Internet.
Which of the following tools is the MOST appropriate to complete the assessment?

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

Answer: D

NEW QUESTION 662
- (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 665
- (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 669
- (Exam Topic 15)
At which phase of the software assurance life cycle should risks associated with software acquisition strategies be identified?

A. Follow-on phase
B. Planning phase
C. Monitoring and acceptance phase
D. Contracting phase

Answer: C

NEW QUESTION 671
- (Exam Topic 15)
A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

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

Answer: D

NEW QUESTION 674
- (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 677
- (Exam Topic 15)
In an IDEAL encryption system, who has sole access to the decryption key?

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

Answer: B

NEW QUESTION 678
- (Exam Topic 15)
Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

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

Answer: B

NEW QUESTION 682
- (Exam Topic 15)
A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several ‘open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

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

Answer: C

NEW QUESTION 684
- (Exam Topic 15)
Which of the following is a secure design principle for a new product?

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

Answer: A

NEW QUESTION 685
- (Exam Topic 15)
The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

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

Answer: A

NEW QUESTION 687
- (Exam Topic 15)
What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

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

Answer: D

NEW QUESTION 688
- (Exam Topic 15)
Which of the following is the MAIN benefit of off-site storage?

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

Answer: A

NEW QUESTION 689
- (Exam Topic 14)
Which of the following is the BEST technique to facilitate secure software development?

A. Adhere to secure coding practices for the software application under development.
B. Conduct penetrating testing for the software application under development.
C. Develop a threat modeling review for the software application under development.
D. Perform a code review process for the software application under development.

Answer: A

NEW QUESTION 692
- (Exam Topic 14)
Which of the following is the MOST important consideration that must be taken into account when deploying an enterprise patching solution that includes mobile devices?

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

Answer: C

NEW QUESTION 695
- (Exam Topic 14)
What steps can be taken to prepare personally identifiable information (PII) for processing by a third party?

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

Answer: C

NEW QUESTION 698
- (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 702
- (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 707
- (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 712
- (Exam Topic 14)
What protocol is often used between gateway hosts on the Internet' To control the scope of a Business Continuity Management (BCM) system, a security practitioner should identify which of the following?

A. Size, nature, and complexity of the organization
B. Business needs of the security organization
C. All possible risks
D. Adaptation model for future recovery planning

Answer: B

NEW QUESTION 717
- (Exam Topic 14)
An organization wants to enable uses to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (F1M). Which of the following is used behind the scenes in a FIM deployment?

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

Answer: C

NEW QUESTION 718
- (Exam Topic 14)
Continuity of operations is BEST supported by which of the following?

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

Answer: B

NEW QUESTION 723
- (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 726
- (Exam Topic 14)
Internet protocol security (IPSec), point-to-point tunneling protocol (PPTP), and secure sockets Layer (SSL) all use Which of the following to prevent replay attacks?

A. Large Key encryption
B. Single integrity protection
C. Embedded sequence numbers
D. Randomly generated nonces

Answer: C

NEW QUESTION 729
- (Exam Topic 14)
Which of the following techniques is effective to detect taps in fiber optic cables?

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

Answer: B

NEW QUESTION 731
- (Exam Topic 14)
Which of the following value comparisons MOST accurately reflects the agile development approach?

A. Processes and toots over individuals and interactions

B. Contract negotiation over customer collaboration
C. Following a plan over responding to change
D. Working software over comprehensive documentation

Answer: D

NEW QUESTION 735
- (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 740
- (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 743
- (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 748
- (Exam Topic 14)
Functional security testing is MOST critical during which phase of the system development life cycle (SDLC)?

A. Operations / Maintenance
B. Implementation
C. Acquisition / Development
D. Initiation

Answer: B

NEW QUESTION 753
- (Exam Topic 14)
A corporate security policy specifies that all devices on the network must have updated operating system patches and anti-malware software. Which technology should be used to enforce this policy?

A. Network Address Translation (NAT)
B. Stateful Inspection
C. Packet filtering
D. Network Access Control (NAC)

Answer: D

NEW QUESTION 755
- (Exam Topic 14)
Which of the following is a MAJOR concern when there is a need to preserve or retain information for future retrieval?

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

Answer: C

NEW QUESTION 758
- (Exam Topic 14)
When adopting software as a service (Saas), which security responsibility will remain with remain with the adopting organization?

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

Answer: B

NEW QUESTION 762
- (Exam Topic 14)
Which of the following types of data would be MOST difficult to detect by a forensic examiner?

A. Slack space data
B. Steganographic data
C. File system deleted data
D. Data stored with a different file type extension

Answer: C

NEW QUESTION 766
- (Exam Topic 14)
Which is the MOST critical aspect of computer-generated evidence?

A. Objectivity
B. Integrity
C. Timeliness
D. Relevancy

Answer: B

NEW QUESTION 767
- (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 771
- (Exam Topic 14)
Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

A. Data access control policies
B. Threat modeling
C. Common Criteria (CC)
D. Business Impact Analysis (BIA)

Answer: A

NEW QUESTION 775
- (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 777
- (Exam Topic 14)
Which of the following is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services?

A. The acquiring organization
B. The service provider
C. The risk executive (function)
D. The IT manager

Answer: C

NEW QUESTION 780
- (Exam Topic 14)
Which of the following is the MOST effective countermeasure against Man-in-the Middle (MITM) attacks while using online banking?

A. Transport Layer Security (TLS)
B. Secure Sockets Layer (SSL)
C. Pretty Good Privacy (PGP)
D. Secure Shell (SSH)

Answer: A

NEW QUESTION 785
- (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 790
- (Exam Topic 14)
Which of the following is the final phase of the identity and access provisioning lifecycle?

A. Recertification
B. Revocation
C. Removal
D. Validation

Answer: B

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

NEW QUESTION 792
- (Exam Topic 14)
From an asset security perspective, what is the BEST countermeasure to prevent data theft due to data remanence when a sensitive data storage media is no longer needed?

A. Return the media to the system owner.
B. Delete the sensitive data from the media.
C. Physically destroy the retired media.
D. Encrypt data before it Is stored on the media.

Answer: C

NEW QUESTION 795
- (Exam Topic 14)
An organization discovers that its secure file transfer protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization's general information technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.
Which of the following is the MOST probable attack vector used in the security breach?

A. Buffer overflow
B. Weak password able to lack of complexity rules
C. Distributed Denial of Service (DDoS)
D. Cross-Site Scripting (XSS)

Answer: A

NEW QUESTION 800
- (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 805
- (Exam Topic 14)
Which layer of the Open system Interconnect (OSI) model is responsible for secure data transfer between applications, flow control, and error detection and correction?

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

Answer: B

NEW QUESTION 808
- (Exam Topic 14)
Which of the following is the BEST defense against password guessing?

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

Answer: D

NEW QUESTION 813
- (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 814
- (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 815
- (Exam Topic 14)
An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.
Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

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

Answer: A

NEW QUESTION 820
- (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 821
- (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 823
- (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 827
- (Exam Topic 14)
A security architect is responsible for the protection of a new home banking system. Which of the following solutions can BEST improve the confidentiality and integrity of this external system?

A. Intrusion Prevention System (IPS)
B. Denial of Service (DoS) protection solution
C. One-time Password (OTP) token
D. Web Application Firewall (WAF)

Answer: A

NEW QUESTION 830
- (Exam Topic 14)
How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

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

Answer: A

NEW QUESTION 831
- (Exam Topic 14)
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

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

Answer: C

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

NEW QUESTION 832
- (Exam Topic 14)
Which of the following is a PRIMARY challenge when running a penetration test?

A. Determining the cost
B. Establishing a business case
C. Remediating found vulnerabilities
D. Determining the depth of coverage

Answer: D

NEW QUESTION 833
- (Exam Topic 14)
Which of the following models uses unique groups contained in unique conflict classes?

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

Answer: C

NEW QUESTION 838
- (Exam Topic 14)
According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

A. Level 0: Incomplete
B. Level 1: Performed
C. Level 2: Managed
D. Level 3: Defined

Answer: D

NEW QUESTION 841
- (Exam Topic 14)
In fault-tolerant systems, what do rollback capabilities permit?

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

Answer: A

NEW QUESTION 844
.....

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