ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 15)
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 3
- (Exam Topic 15)
An organization plans to acquire @ commercial off-the-shelf (COTS) system to replace their aging home-built reporting system. When should the organization's security team FIRST get involved in this acquisition's life cycle?

A. When the system is being designed, purchased, programmed, developed, or otherwise constructed
B. When the system is verified and validated
C. When the system is deployed into production
D. When the need for a system is expressed and the purpose of the system Is documented

Answer: D

NEW QUESTION 4
- (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 5
- (Exam Topic 15)
Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 15)
Which of the following is an important requirement when designing a secure remote access system?

A. Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated.
B. Provide privileged access rights to computer files and systems.
C. Ensure that logging and audit controls are included.
D. Reduce administrative overhead through password self service.

Answer: C

NEW QUESTION 7
- (Exam Topic 15)
Which of the following is the top barrier for companies to adopt cloud technology?

A. Migration period
B. Data integrity
C. Cost

D. Security

Answer: D

NEW QUESTION 8
- (Exam Topic 15)
Wireless users are reporting intermittent Internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time.
The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

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

Answer: A

NEW QUESTION 9
- (Exam Topic 15)
Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless
Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 15)
A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

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

Answer: B

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

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

Answer: A

NEW QUESTION 14
- (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 16
- (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 21

- (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 23
- (Exam Topic 15)
Which of the following is established to collect information Se eee ee ee nation readily available in part through implemented security controls?

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

Answer: D

NEW QUESTION 26
- (Exam Topic 15)
A large human resources organization wants to integrate their identity management with a trusted partner organization. The human resources organization wants to maintain the creation and management of the identities and may want to share with other partners in the future. Which of the following options BEST serves their needs?

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

Answer: A

NEW QUESTION 28
- (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 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 35
- (Exam Topic 15)
Which of the following is a common term for log reviews, synthetic transactions, and code reviews?

A. Security control testing
B. Application development
C. Spiral development functional testing
D. DevOps Integrated Product Team (IPT) development

Answer: B

NEW QUESTION 38
- (Exam Topic 15)
When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

A. SOC 1 Type 1

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

Answer: C

NEW QUESTION 40
- (Exam Topic 15)
Which of the following is the BEST way to protect an organization's data assets?

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

Answer: B

NEW QUESTION 43
- (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 47
- (Exam Topic 15)
What type of database attack would allow a customer service employee to determine quarterly sales results
before they are publically announced?

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

Answer: A

NEW QUESTION 52
- (Exam Topic 15)
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 56
- (Exam Topic 15)
Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

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

Answer: A

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

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

Answer: D

NEW QUESTION 60

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

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

Answer: D

NEW QUESTION 63
- (Exam Topic 15)
What is the 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 65
- (Exam Topic 15)
Which of the following is the MOST effective preventative method to identify security flaws in software?

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

Answer: B

NEW QUESTION 69
- (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 72
- (Exam Topic 15)
Which of the following is the BEST way to protect against Structured Query language (SQL) injection?

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

Answer: D

NEW QUESTION 77
- (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 80
- (Exam Topic 15)
Which of the following statements BEST distinguishes a stateful packet inspection firewall from a stateless packet filter firewall?

A. The SPI inspects the flags on Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets.
B. The SPI inspects the traffic in the context of a session.
C. The SPI is capable of dropping packets based on a pre-defined rule set.
D. The SPI inspects traffic on a packet-by-packet basis.

Answer: B

NEW QUESTION 81
- (Exam Topic 15)
Which of the following uses the destination IP address to forward packets?

A. A bridge
B. A Layer 2 switch
C. A router
D. A repeater

Answer: C

NEW QUESTION 85
- (Exam Topic 15)
Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

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

Answer: D

NEW QUESTION 86
- (Exam Topic 15)
What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

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

Answer: A

NEW QUESTION 90
- (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 93
- (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 94
- (Exam Topic 15)
Which element of software supply chain management has the GREATEST security risk to organizations?

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

Answer: B

NEW QUESTION 96
- (Exam Topic 15)
Which of the following is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions?

A. Information Security Management System (ISMS)
B. Information Sharing & Analysis Centers (ISAC)

C. Risk Management Framework (RMF)
D. Information Security Continuous Monitoring (ISCM)

Answer: D

NEW QUESTION 98
- (Exam Topic 15)
As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem?

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

Answer: C

NEW QUESTION 100
- (Exam Topic 15)

A. Require the cloud 1AM provider to use declarative security instead of programmatic authentication checks.
B. Integrate a Web-Application Firewall (WAF) In reverie-proxy mode in front of the service provider.
C. Apply Transport layer Security (TLS) to the cloud-based authentication checks.
D. Install an on-premise Authentication Gateway Service (AGS) In front of the service provider.

Answer: D

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

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

Answer: B

NEW QUESTION 103
- (Exam Topic 15)
A financial services organization has employed a security consultant to review processes used by employees across various teams. The consultant interviewed a member of the application development practice and found gaps in their threat model. Which of the following correctly represents a trigger for when a threat model should be revised?

A. A new data repository is added.
B. is After operating system (OS) patches are applied
C. After a modification to the firewall rule policy
D. A new developer is hired into the team.

Answer: D

NEW QUESTION 108
- (Exam Topic 15)
A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

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

Answer: D

NEW QUESTION 111

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

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

Answer: B

NEW QUESTION 116
- (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 119
- (Exam Topic 15)
Spyware is BEST described as

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

Answer: B

NEW QUESTION 121
- (Exam Topic 15)
When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

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

Answer: C

NEW QUESTION 126
- (Exam Topic 15)
Which of the following is included in change management?

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

Answer: A

NEW QUESTION 127
- (Exam Topic 15)
Which of the following is the MOST common cause of system or security failures?

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

Answer: D

NEW QUESTION 130
- (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 135
- (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 136
- (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 138
- (Exam Topic 15)
What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

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

Answer: A

NEW QUESTION 143
- (Exam Topic 15)
Which of the following is the MOST effective countermeasure against data remanence?

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

Answer: A

NEW QUESTION 146
- (Exam Topic 15)
Which of the following determines how traffic should flow based on the status of the infrastructure layer?

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

Answer: A

NEW QUESTION 149
- (Exam Topic 15)
Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management
decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

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

Answer: A

NEW QUESTION 151
- (Exam Topic 15)

Which of the following is the MOST comprehensive Business Continuity (BC) test?

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

Answer: C

NEW QUESTION 156
- (Exam Topic 15)
Which of the following BEST represents a defense in depth concept?

A. Network-based data loss prevention (DLP), Network Access Control (NAC), network-based Intrusion prevention system (NIPS), Port security on core switches
B. Host-based data loss prevention (DLP), Endpoint anti-malware solution, Host-based integrity checker, Laptop locks, hard disk drive (HDD) encryption
C. Endpoint security management, network intrusion detection system (NIDS), Network Access Control (NAC), Privileged Access Management (PAM), security information and event management (SIEM)
D. Web application firewall (WAF), Gateway network device tuning, Database firewall, Next-Generation Firewall (NGFW), Tier-2 demilitarized zone (DMZ) tuning

Answer: C

NEW QUESTION 157
- (Exam Topic 15)
Which of the following is an open standard for exchanging authentication and authorization data between parties?

A. Wired markup language
B. Hypertext Markup Language (HTML)
C. Extensible Markup Language (XML)
D. Security Assertion Markup Language (SAML)

Answer: D

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

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

Answer: A

NEW QUESTION 163
- (Exam Topic 15)
Which of the following are the B EST characteristics of security metrics?

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

Answer: D

NEW QUESTION 166
- (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 167
- (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 169
- (Exam Topic 15)
A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

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

Answer: A

NEW QUESTION 170
- (Exam Topic 15)
Which of the following is a Key Performance Indicator (KPI) for a security training and awareness program?

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

Answer: B

NEW QUESTION 172
- (Exam Topic 15)
Computer forensics requires which of the following MAIN steps?

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

Answer: B

NEW QUESTION 173
- (Exam Topic 15)
Which of the following is the MOST appropriate control for asset data labeling procedures?

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

Answer: C

NEW QUESTION 176
- (Exam Topic 15)
An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

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

Answer: D

NEW QUESTION 179
- (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 183
- (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 186
- (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 190
- (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 194
- (Exam Topic 15)
Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

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

Answer: C

NEW QUESTION 197
- (Exam Topic 15)
In systems security engineering, what does the security principle of modularity provide?

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

Answer: A

NEW QUESTION 200
- (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 201
- (Exam Topic 15)
When assessing the audit capability of an application, which of the following activities is MOST important?

A. Determine if audit records contain sufficient information.
B. Review security plan for actions to be taken in the event of audit failure.
C. Verify if sufficient storage is allocated for audit records.
D. Identify procedures to investigate suspicious activity.

Answer: C

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

A. White box testing

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

Answer: C

NEW QUESTION 207
- (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 212
- (Exam Topic 15)
After the INITIAL input o f a user identification (ID) and password, what is an authentication system that prompts the user for a different response each time the user logs on?

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

Answer: C

NEW QUESTION 215
- (Exam Topic 15)
An organization has discovered that organizational data is posted by employees to data storage accessible to the general public. What is the PRIMARY step an organization must take
to ensure data is properly protected from public release?

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

Answer: C

NEW QUESTION 220
- (Exam Topic 15)
An information security administrator wishes to block peer-to-peer (P2P) traffic over Hypertext Transfer Protocol (HTTP) tunnels. Which of the following layers of the Open Systems Interconnection (OSI) model requires inspection?

A. Presentation
B. Transport
C. Session
D. Application

Answer: A

NEW QUESTION 222
- (Exam Topic 15)
A security professional has been assigned to assess a web application. The assessment report recommends switching to Security Assertion Markup Language (SAML). What is the PRIMARY security benefit in switching to SAML?

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

Answer: B

NEW QUESTION 224
- (Exam Topic 15)
Which of the following is the MOST significant key management problem due to the number of keys created?

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

Answer: B

NEW QUESTION 229
- (Exam Topic 15)
A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

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

Answer: D

NEW QUESTION 234
- (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 236
- (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 241
- (Exam Topic 15)
Security Software Development Life Cycle (SDLC) expects application code to be written In a consistent manner to allow ease of auditing and which of the following?

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

Answer: A

NEW QUESTION 242
- (Exam Topic 15)
A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

A. Read
B. Execute
C. Write
D. Append

Answer: C

NEW QUESTION 246
- (Exam Topic 15)
Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

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

Answer: C

NEW QUESTION 249
- (Exam Topic 15)
Which of the following is the PRIMARY issue when analyzing detailed log information?

A. Logs may be unavailable when required
B. Timely review of the data is potentially difficult

C. Most systems and applications do not support logging
D. Logs do not provide sufficient details of system and individual activities

Answer: D

NEW QUESTION 252
- (Exam Topic 15)
Which of the following is the PRIMARY purpose of due diligence when an organization embarks on a merger or acquisition?

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

Answer: A

NEW QUESTION 253
- (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 257
- (Exam Topic 15)
What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

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

Answer: C

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

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

Answer: A

NEW QUESTION 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)
At the destination host, which of the following OSI model layers will discard a segment with a bad checksum
in the UDP header?

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

Answer: C

NEW QUESTION 273
- (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 276
- (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 277
- (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 282
- (Exam Topic 15)
Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

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

Answer: B

NEW QUESTION 283
- (Exam Topic 15)
When conducting a third-party risk assessment of a new supplier, which of the following reports should be reviewed to confirm the operating effectiveness of the
security, availability, confidentiality, and privacy trust principles?

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

Answer: B

NEW QUESTION 288
- (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 291
- (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 296
- (Exam Topic 15)
Which of the following vulnerability assessment activities BEST exemplifies the Examine method of assessment?

A. Ensuring that system audit logs capture all relevant data fields required by the security controls baseline
B. Performing Port Scans of selected network hosts to enumerate active services
C. Asking the Information System Security Officer (ISSO) to describe the organization's patch management processes
D. Logging into a web server using the default administrator account and a default password

Answer: D

NEW QUESTION 297
- (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 300
- (Exam Topic 15)
Which of the following is considered the FIRST step when designing an internal security control assessment?

A. Create a plan based on recent vulnerability scans of the systems in question.
B. Create a plan based on comprehensive knowledge of known breaches.
C. Create a plan based on a recognized framework of known controls.
D. Create a plan based on reconnaissance of the organization's infrastructure.

Answer: D

NEW QUESTION 303
- (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 306
- (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:

NEW QUESTION 308
- (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 312
- (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 314
- (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 316
- (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 318
- (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 323
- (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 324
- (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 327
- (Exam Topic 15)
A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

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

Answer: D

NEW QUESTION 329
- (Exam Topic 15)
Upon commencement of an audit within an organization, which of the following actions is MOST important for the auditor(s) to take?

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

Answer: C

NEW QUESTION 333
- (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 335
- (Exam Topic 15)
What Hypertext Transfer Protocol (HTTP) response header can be used to disable the execution of inline JavaScript and the execution of eval()-type functions?

A. Strict-Transport-Security
B. X-XSS-Protection
C. X-Frame-Options
D. Content-Security-Policy

Answer: D

NEW QUESTION 337
- (Exam Topic 15)
Configuring a Wireless Access Point (WAP) with the same Service Set Identifier (SSID) as another WAP in order to have users unknowingly connect is referred to as which of the following?

A. Jamming
B. Man-irHht-Middk (MITM)
C. War driving
D. Internet Protocol (IP) spoofing

Answer: B

NEW QUESTION 338
- (Exam Topic 15)
Which of the following is a key responsibility for a data steward assigned to manage an enterprise data lake?

A. Ensure proper business definition, value, and usage of data collected and stored within the enterprise data lake.
B. Ensure proper and identifiable data owners for each data element stored within an enterprise data lake.
C. Ensure adequate security controls applied to the enterprise data lake.
D. Ensure that any data passing within remit is being used in accordance with the rules and regulations of the business.

Answer: A

NEW QUESTION 343

- (Exam Topic 15)
An access control list (ACL) on a router is a feature MOST similar to which type of firewall?

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

Answer: B

NEW QUESTION 346
- (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 347
- (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 352
- (Exam Topic 15)
Which of the following is a correct feature of a virtual local area network (VLAN)?

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

Answer: A

NEW QUESTION 357
- (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 361
- (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 364
- (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 367
- (Exam Topic 15)
An organization wants to share data securely with their partners via the Internet. Which standard port is typically used to meet this requirement?

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

Answer: C

NEW QUESTION 372
- (Exam Topic 15)
Which of the following are the three MAIN categories of security controls?

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

Answer: A

NEW QUESTION 374
- (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 379
- (Exam Topic 15)
When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of big data?

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

Answer: C

NEW QUESTION 382
- (Exam Topic 15)
Which of the following documents specifies services from the client's viewpoint?

A. Service level report
B. Business impact analysis (BIA)
C. Service level agreement (SLA)
D. Service Level Requirement (SLR)

Answer: C

NEW QUESTION 383
- (Exam Topic 15)
Which of the following statements is TRUE about Secure Shell (SSH)?

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

Answer: B

NEW QUESTION 388
- (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 389
- (Exam Topic 15)
Which of the following is the MOST effective measure for dealing with rootkit attacks?

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

Answer: D

NEW QUESTION 392
- (Exam Topic 15)
Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

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

Answer: C

NEW QUESTION 395
- (Exam Topic 15)
Which of the following is the MOST important first step in preparing for a security audit?

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

Answer: B

NEW QUESTION 396
- (Exam Topic 15)
Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

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

Answer: C

NEW QUESTION 400
- (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 403
- (Exam Topic 15)
The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

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

Answer: D

NEW QUESTION 408
- (Exam Topic 15)
Of the following, which BEST provides non- repudiation with regards to access to a server room?

A. Fob and Personal Identification Number (PIN)
B. Locked and secured cages
C. Biometric readers

D. Proximity readers

Answer: C

NEW QUESTION 413
- (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 415
- (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 418
- (Exam Topic 15)
Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

A. Audit
B. Compliance
C. Legal
D. Security

Answer: C

NEW QUESTION 419
- (Exam Topic 15)
Which of the following BEST describes the purpose of Border Gateway Protocol (BGP)?

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

Answer: B

NEW QUESTION 420
- (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?
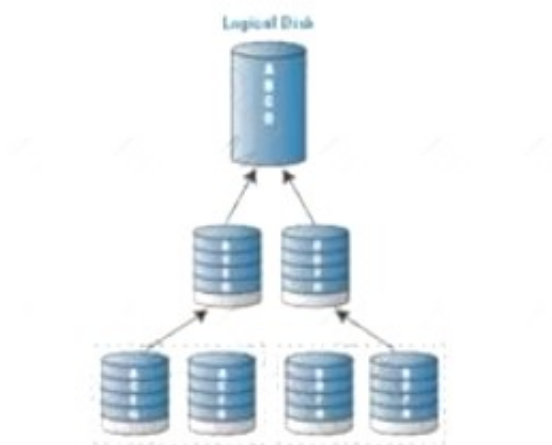
A. nslookup
B. netstat -a
C. ipeonfig /a
D. arp -a

Answer: B

NEW QUESTION 424
- (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 425
- (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 427
- (Exam Topic 15)
a large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.
What is this value called?

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

Answer: C

NEW QUESTION 432
- (Exam Topic 15)
An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data protection methods.
Which of the following is the BEST data protection method?

A. Encryption
B. Backups
C. Data obfuscation
D. Strong authentication

Answer: C

NEW QUESTION 435
- (Exam Topic 15)
An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 1
B. 2
C. 3

Answer: A

NEW QUESTION 439
- (Exam Topic 15)
Which software defined networking (SDN) architectural component is responsible for translating network requirements?

A. SDN Application
B. SDN Data path
C. SDN Controller

D. SDN Northbound Interfaces

Answer: D

NEW QUESTION 443
- (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 445
- (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 449
- (Exam Topic 15)
An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weal

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

Answer: A

NEW QUESTION 451
- (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 456
- (Exam Topic 15)
What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

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

Answer: C

NEW QUESTION 459
- (Exam Topic 15)
What is the second phase of public key infrastructure (PKI) key/certificate life-cycle management?

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

Answer: A

NEW QUESTION 464
- (Exam Topic 15)

Which of the following vulnerabilities can be BEST detected using automated analysis?

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

Answer: D

NEW QUESTION 469
- (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 472
- (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 475
- (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 477
- (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 481
- (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 482
- (Exam Topic 15)
An Internet media company produces and broadcasts highly popular television shows. The company is suffering a huge revenue loss due to piracy. What technique should be used to track the distribution of content?

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

Answer: D

NEW QUESTION 484
- (Exam Topic 15)
Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

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

Answer: C

NEW QUESTION 487
- (Exam Topic 15)
A firm within the defense industry has been directed to comply with contractual requirements for encryption of a government client's Controlled Unclassified Information (CUI). What encryption strategy represents how to protect data at rest in the MOST efficient and cost-effective manner?

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

Answer: C

NEW QUESTION 492
- (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 497
- (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 498
- (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 500
- (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 505
- (Exam Topic 15)
The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery. Which of the following is the
MOST challenging aspect of this investigation?

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

Answer: C

NEW QUESTION 508
- (Exam Topic 15)
A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging generates extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

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

Answer: D

NEW QUESTION 509
- (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 513
- (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 517
- (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 521
- (Exam Topic 15)
What is the PRIMARY objective of the post-incident phase of the incident response process in the security operations center (SOC)?

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

Answer: A

NEW QUESTION 524
- (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 528
- (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 531
- (Exam Topic 15)
In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

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

Answer: D

NEW QUESTION 535
- (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 539
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a
particular system over a 12-month period. Which type of SOC report should be utilized?

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

Answer: C

NEW QUESTION 540
- (Exam Topic 15)
What is the BEST design for securing physical perimeter protection?

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

Answer: B

NEW QUESTION 544
- (Exam Topic 15)
What is a security concern when considering implementing software-defined networking (SDN)?

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

Answer: C

NEW QUESTION 549
- (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 553
- (Exam Topic 15)
A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

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

Answer: C

NEW QUESTION 557
- (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 560
- (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 563
- (Exam Topic 15)
A security professional is assessing the risk in an application and does not take into account any mitigating or compensating controls. This type of risk rating is an example of which of the following?

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

Answer: B

NEW QUESTION 565
- (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 568
- (Exam Topic 15)
Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

A. Payload encryption
B. Sender confidentiality
C. Sender non-repudiation
D. Multi-factor authentication (MFA)

Answer: C

NEW QUESTION 569
- (Exam Topic 15)
How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

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

Answer: C

NEW QUESTION 570
- (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 571
- (Exam Topic 15)
An application developer receives a report back from the security team showing their automated tools were able to successfully enter unexpected data into the
organization's customer service portal, causing the site to crash. This is an example of which type of testing?

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

Answer: D

NEW QUESTION 576
- (Exam Topic 15)
Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?\

A. System logs
B. Anti-spyware
C. Integrity checker
D. Firewall logs

Answer: C

NEW QUESTION 577
- (Exam Topic 15)
In an environment where there is not full administrative control over all network connected endpoints, such as a university where non-corporate devices are used,
what is
the BEST way to restrict access to the network?

A. Use switch port security to limit devices connected to a particular switch port.
B. Use of virtual local area networks (VLAN) to segregate users.
C. Use a client-based Network Access Control (NAC) solution.
D. Use a clientless Network Access Control (NAC) solution

Answer: A

NEW QUESTION 579
- (Exam Topic 15)
The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-
critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in
which role in order to ensure proper protection of data during and after the cloud migration?

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

Answer: A

NEW QUESTION 580
- (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 581
- (Exam Topic 15)
What part of an organization's strategic risk assessment MOST likely includes information on items affecting the success of the organization?

A. Key Risk Indicator (KRI)
B. Threat analysis
C. Vulnerability analysis
D. Key Performance Indicator (KPI)

Answer: A

NEW QUESTION 585
- (Exam Topic 15)
What is the MOST common cause of Remote Desktop Protocol (RDP) compromise?

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

Answer: B

NEW QUESTION 586
- (Exam Topic 15)
Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

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

Answer: C

NEW QUESTION 588
- (Exam Topic 15)
An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a
per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

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

Answer: A

NEW QUESTION 590
- (Exam Topic 15)
In Federated Identity Management (FIM), which of the following represents the concept of federation?

A. Collection of information logically grouped into a single entity
B. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications
C. Collection of information for common identities in a system
D. Collection of domains that have established trust among themselves

Answer: D

NEW QUESTION 594
- (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 596
- (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 599
- (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 602
- (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 604
- (Exam Topic 15)
The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a
level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

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

Answer: D

NEW QUESTION 607
- (Exam Topic 15)
When MUST an organization's information security strategic plan be reviewed?

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

Answer: D

NEW QUESTION 609
- (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 613
- (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 615
- (Exam Topic 15)
Which of the following is the MOST effective strategy to prevent an attacker from disabling a network?

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

Answer: D

NEW QUESTION 617
- (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 621
- (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 624
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

Answer: C

NEW QUESTION 626
- (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 627
- (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 631
- (Exam Topic 15)

Which of the following are all elements of a disaster recovery plan (DRP)?

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

Answer: C

NEW QUESTION 636
- (Exam Topic 15)
What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

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

Answer: D

NEW QUESTION 637
- (Exam Topic 15)
Which of the following BEST describes botnets?

A. Computer systems on the Internet that are set up to trap people who attempt to penetrate other computer system
B. Set of related programs that protects the resources of a private network from other networks
C. Small network inserted in a neutral zone between an organization's private network and the outside public network
D. Groups of computers that are used to launch destructive attacks

Answer: D

NEW QUESTION 639
- (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 640
- (Exam Topic 15)
A security professional has been requested by the Board of Directors and Chief Information Security Officer (CISO) to perform an internal and external penetration test. What is the BEST course of action?

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

Answer: D

NEW QUESTION 644
- (Exam Topic 15)
Building blocks for software-defined networks (SDN) require which of the following?

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

Answer: C

NEW QUESTION 646
- (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 649
- (Exam Topic 14)
What form of attack could this represent?

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

Answer: D

NEW QUESTION 650
- (Exam Topic 14)
Which of the following media is LEAST problematic with data remanence?

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

Answer: A

NEW QUESTION 653
- (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 658
- (Exam Topic 14)
Which one of the following documentation should be included in a Disaster Recovery (DR) package?

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

Answer: C

NEW QUESTION 661
- (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 663
- (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 667
- (Exam Topic 14)
Which of the following is used to support the concept of defense in depth during the development phase of a software product?

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

Answer: B

NEW QUESTION 670
- (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 672
- (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 673
- (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 676
- (Exam Topic 14)
How long should the records on a project be retained?

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

Answer: B

NEW QUESTION 679
- (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 683
- (Exam Topic 14)
Which of the following is a characteristic of the independent testing of a program?

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

Answer: A

NEW QUESTION 688
- (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 689
- (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 692
- (Exam Topic 14)
Which of the following is the GREATEST security risk associated with the user of identity as a service (IDaaS) when an organization its own software?

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

Answer: B

NEW QUESTION 697
- (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 701
- (Exam Topic 14)
Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?

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

Answer: D

NEW QUESTION 704
- (Exam Topic 14)
What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

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

Answer: B

NEW QUESTION 709
- (Exam Topic 14)
Additional padding may be added to toe Encapsulating Security Protocol (ESP) b trailer to provide which of the following?

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

Answer: C

NEW QUESTION 713

- (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 714
- (Exam Topic 14)
How can an attacker exploit overflow to execute arbitrary code?

A. Modify a function's return address.
B. Alter the address of the stack.
C. Substitute elements in the stack.
D. Move the stack pointer.

Answer: A

NEW QUESTION 716
- (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 717
- (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 719
- (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 723
- (Exam Topic 14)
What is the PRIMARY purpose for an organization to conduct a security audit?

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

Answer: A

NEW QUESTION 726
- (Exam Topic 14)
A user downloads a file from the Internet, then applies the Secure Hash Algorithm 3 (SHA-3c?

A. It verifies the integrity of the file.
B. It checks the file for malware.
C. It ensures the entire file downloaded.
D. It encrypts the entire file.

Answer: A

Explanation:

Reference: https://blog.logsign.com/how-to-check-the-integrity-of-a-file/

NEW QUESTION 727
- (Exam Topic 14)
What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

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

Answer: C

NEW QUESTION 730
- (Exam Topic 14)
When dealing with shared, privilaged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

A. Regularity change the passwords,
B. implement a password vaulting solution.
C. Lock passwords in tamperproof envelopes in a safe.
D. Implement a strict access control policy.

Answer: B

NEW QUESTION 731
- (Exam Topic 14)
Which of the following is the PRIMARY consideration when determining the frequency an automated control should be assessed or monitored?

A. The complexity of the automated control
B. The level of automation of the control
C. The range of values of the automated control
D. The volatility of the automated control

Answer: B

NEW QUESTION 734
- (Exam Topic 14)
Which of the following authorization standards is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM)?

A. Security Assertion Markup Language (SAML)
B. Open Authentication (OAUTH)
C. Remote Authentication Dial-in User service (RADIUS)
D. Terminal Access Control Access Control System Plus (TACACS+)

Answer: B

NEW QUESTION 737
- (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 741
- (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 744
- (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 747
- (Exam Topic 14)
Which of the following is the MOST critical success factor in the security patch management process?

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

Answer: A

NEW QUESTION 751
- (Exam Topic 14)
What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

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

Answer: B

NEW QUESTION 755
- (Exam Topic 14)
If a content management system (CSM) is implemented, which one of the following would occur?

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

Answer: A

NEW QUESTION 758
- (Exam Topic 14)
Which of the following job functions MUST be separated to maintain data and application integrity?

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

Answer: D

NEW QUESTION 763
- (Exam Topic 14)
Which of the following open source software issues pose the MOST risk to an application?

A. The software is beyond end of life and the vendor is out of business.
B. The software is not used or popular in the development community.
C. The software has multiple Common Vulnerabilities and Exposures (CVE) and only some are remediated.
D. The software has multiple Common Vulnerabilities and Exposures (CVE) but the CVEs are classified as low risks.

Answer: D

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

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

Answer: D

NEW QUESTION 768
- (Exam Topic 14)
What is the MOST effective way to protect privacy?

A. Eliminate or reduce collection of personal information.
B. Encrypt all collected personal information.
C. Classify all personal information at the highest information classification level.
D. Apply tokenization to all personal information records.

Answer: D

NEW QUESTION 773
- (Exam Topic 14)
Point-to-Point Protocol (PPP) was designed to specifically address what issue?

A. A common design flaw in telephone modems
B. Speed and reliability issues between dial-up users and Internet Service Providers (ISP).
C. Compatibility issues with personal computers and web browsers
D. The security of dial-up connections to remote networks

Answer: B

NEW QUESTION 775
- (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 778
- (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 783
- (Exam Topic 14)
Which of the following would an internal technical security audit BEST validate?

A. Whether managerial controls are in place
B. Support for security programs by executive management
C. Appropriate third-party system hardening
D. Implementation of changes to a system

Answer: D

NEW QUESTION 786
- (Exam Topic 14)
Which of the following is the MOST important activity an organization performs to ensure that securiy is part of the overall organization culture?

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

Answer: C

NEW QUESTION 787
- (Exam Topic 14)
What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

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

Answer: C

NEW QUESTION 790
......

Relate Links

100% Pass Your CISSP Exam with Exambible Prep Materials

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

Contact us

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

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