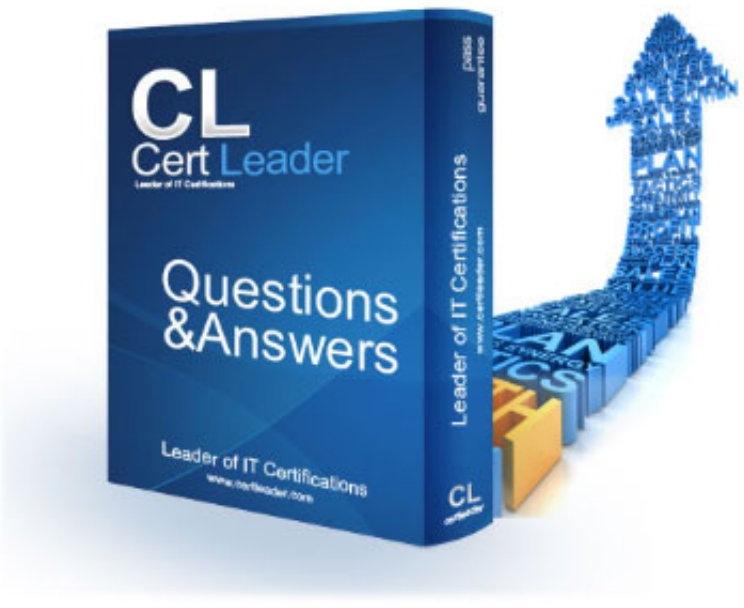
CISSP Dumps

Certified Information Systems Security Professional (CISSP)

https://www.certleader.com/CISSP-dumps.html



NEW QUESTION 1
- (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 2
- (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 3
- (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 4
- (Exam Topic 15)
Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using which protocol?

A. Secure Shell (SSH)
B. Internet Protocol Security (IPsec)
C. Secure Sockets Layer (SSL)
D. Extensible Authentication Protocol (EAP)

Answer: A

NEW QUESTION 5
- (Exam Topic 15)
Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

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

Answer: B

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

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

Answer: A

NEW QUESTION 7
- (Exam Topic 15)
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 8
- (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 9
- (Exam Topic 15)
While reviewing the financial reporting risks of a third-party application, which of the following Service Organization Control (SOC) reports will be the MOST useful?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 15)
Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-systems gracefully handle invalid input?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 15)
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 11
- (Exam Topic 15)
Which of the following is fundamentally required to address potential security issues when initiating software development?

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

Answer: C

NEW QUESTION 12
- (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 13

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

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

Answer: A

NEW QUESTION 19
- (Exam Topic 15)
A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the
BEST design approach to securing this environment?

A. Place firewalls around critical devices, isolating them from the rest of the environment.
B. Layer multiple detective and preventative technologies at the environment perimeter.
C. Use reverse proxies to create a secondary "shadow" environment for critical systems.
D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

Answer: B

NEW QUESTION 20
- (Exam Topic 15)
Which security evaluation model assesses a product's Security Assurance Level (SAL) in comparison to similar solutions?

A. Payment Card Industry Data Security Standard (PCI-DSS)
B. International Organization for Standardization (ISO) 27001
C. Common criteria (CC)
D. Control Objectives for Information and Related Technology (COBIT)

Answer: C

NEW QUESTION 21
- (Exam Topic 15)
Which of the following provides the MOST secure method for Network Access Control (NAC)?

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

Answer: B

NEW QUESTION 25
- (Exam Topic 15)
During a penetration test, what are the three PRIMARY objectives of the planning phase?

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

Answer: D

NEW QUESTION 28
- (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 29
- (Exam Topic 15)
In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed?

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

Answer: D

NEW QUESTION 30
- (Exam Topic 15)
To minimize the vulnerabilities of a web-based application, which of the following FIRST actions will lock down the system and minimize the risk of an attack?

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

Answer: D

NEW QUESTION 35
- (Exam Topic 15)
An organization wants to define its physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

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

Answer: A

NEW QUESTION 37
- (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 42
- (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 47
- (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 51
- (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 55
- (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)
What is the MAIN purpose of conducting a business impact analysis (BIA)?

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

Answer: B

NEW QUESTION 57
- (Exam Topic 15)
An organization needs a general purpose document to prove that its internal controls properly address security, availability, processing integrity, confidentiality or privacy risks. Which of the following reports is required?

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

Answer: C

NEW QUESTION 61
- (Exam Topic 15)
Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

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

Answer: B

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

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

Answer: D

NEW QUESTION 66
- (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 69
- (Exam Topic 15)
What is the PRIMARY benefit of incident reporting and computer crime investigations?

A. Providing evidence to law enforcement
B. Repairing the damage and preventing future occurrences
C. Appointing a computer emergency response team
D. Complying with security policy

Answer: D

NEW QUESTION 71
- (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 76
- (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 78
- (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 79
- (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 84
- (Exam Topic 15)
Which access control method is based on users issuing access requests on system resources, features assigned to those resources, the operational or situational context, and a set of policies specified in terms of those features and context?

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

Answer: B

NEW QUESTION 86
- (Exam Topic 15)
In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

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

Answer: B

NEW QUESTION 88
- (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 93
- (Exam Topic 15)
A user is allowed to access the file labeled “Financial Forecast,” but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

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

Answer: B

NEW QUESTION 96
- (Exam Topic 15)
Which of the following is an indicator that a company's new user security awareness training module has been effective?

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

Answer: B

NEW QUESTION 101
- (Exam Topic 15)
Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users internal control over financial reporting?

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

Answer: B

NEW QUESTION 104
- (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 108
- (Exam Topic 15)
Which of the following is security control volatility?

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

Answer: D

NEW QUESTION 111

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

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

Answer: D

NEW QUESTION 114
- (Exam Topic 15)
Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

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

Answer: A

NEW QUESTION 119
- (Exam Topic 15)
Which of the following is the MOST important rule for digital investigations?

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

Answer: C

NEW QUESTION 122
- (Exam Topic 15)
Using the cipher text and resultant clear text message to derive the non-alphabetic cipher key is an example of which method of cryptanalytic attack?

A. Frequency analysis
B. Ciphertext-only attack
C. Probable-plaintext attack
D. Known-plaintext attack

Answer: D

NEW QUESTION 123
- (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 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 128
- (Exam Topic 15)
Which of the following are mandatory canons for the (ISC)* Code of Ethics?

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

Answer: D

NEW QUESTION 132
- (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 135
- (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 140
- (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 142
- (Exam Topic 15)
Which of the following goals represents a modern shift in risk management according to National Institute of Standards and Technology (NIST)?

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

Answer: C

NEW QUESTION 147
- (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 148
- (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 153
- (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 156
- (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 161
- (Exam Topic 15)

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

Answer: D

NEW QUESTION 163
- (Exam Topic 15)
Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

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

Answer: B

NEW QUESTION 164
- (Exam Topic 15)
Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

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

Answer: D

NEW QUESTION 169
- (Exam Topic 15)
Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

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

Answer: B

NEW QUESTION 174
- (Exam Topic 15)
In software development, which of the following entities normally signs the code to protect the code integrity?

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

Answer: B

NEW QUESTION 178
- (Exam Topic 15)
Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

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

Answer: B

NEW QUESTION 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 185
- (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 188
- (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 190
- (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 194
- (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 199
- (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 200

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

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

Answer: C

NEW QUESTION 202
- (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 205
- (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 206
- (Exam Topic 15)
In a multi-tenant cloud environment, what approach will secure logical access to assets?

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

Answer: D

NEW QUESTION 207
- (Exam Topic 15)
An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

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

Answer: B

NEW QUESTION 211
- (Exam Topic 15)
Which of the following will accomplish Multi-Factor Authentication (MFA)?

A. Issuing a smart card with a user-selected Personal Identification Number (PIN)
B. Requiring users to enter a Personal Identification Number (PIN) and a password
C. Performing a palm and retinal scan
D. Issuing a smart card and a One Time Password (OTP) token

Answer: A

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

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

Answer: C

NEW QUESTION 218
- (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 219
- (Exam Topic 15)
An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

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

Answer: D

NEW QUESTION 221
- (Exam Topic 15)
What is the FINAL step in the waterfall method for contingency planning?

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

Answer: A

NEW QUESTION 224
- (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 227
- (Exam Topic 15)
What is static analysis intended to do when analyzing an executable file?

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

Answer: D

NEW QUESTION 232

- (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 235
- (Exam Topic 15)
A hospital has allowed virtual private networking (VPN) access to remote database developers. Upon auditing the internal firewall configuration, the network administrator discovered that split-tunneling was enabled. What is the concern with this configuration?

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

Answer: C

NEW QUESTION 237
- (Exam Topic 15)
What is the benefit of using Network Admission Control (NAC)?

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

Answer: C

NEW QUESTION 241
- (Exam Topic 15)
Which of the following outsourcing agreement provisions has the HIGHEST priority from a security operations perspective?

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

Answer: D

NEW QUESTION 243
- (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 246
- (Exam Topic 15)
Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

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

Answer: D

NEW QUESTION 249
- (Exam Topic 15)
An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

A. Default the user to not share any information.

B. Inform the user of the sharing feature changes after implemented.
C. Share only what the organization decides is best.
D. Stop sharing data with the other users.

Answer: D

NEW QUESTION 253
- (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 258
- (Exam Topic 15)
What documentation is produced FIRST when performing an effective physical loss control process?

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

Answer: C

NEW QUESTION 260
- (Exam Topic 15)
Which of the following is the PRIMARY goal of logical access controls?

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

Answer: C

NEW QUESTION 265
- (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 266
- (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 271
- (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 275

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

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

Answer: B

NEW QUESTION 279
- (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 283
- (Exam Topic 15)
A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

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

Answer: C

NEW QUESTION 284
- (Exam Topic 15)
Which of the following explains why classifying data is an important step in performing a Risk assessment?

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

Answer: D

NEW QUESTION 286
- (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 287
- (Exam Topic 15)
According to the (ISC)? ethics canon “act honorably, honestly, justly, responsibly, and legally," which order should be used when resolving conflicts?

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

Answer: A

NEW QUESTION 290
- (Exam Topic 15)
The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

A. Removal of service accounts from review
B. Segregation of Duties (SoD)

C. Clear provisioning policies
D. Frequent audits

Answer: C

NEW QUESTION 291
- (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 294
- (Exam Topic 15)
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

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

Answer: A

NEW QUESTION 296
- (Exam Topic 15)
Which of the following types of datacenter architectures will MOST likely be used in a large SDN and can be extended beyond the datacenter?

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

Answer: B

NEW QUESTION 300
- (Exam Topic 15)
Which of the following types of hosts should be operating in the demilitarized zone (DMZ)?

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

Answer: A

NEW QUESTION 302
- (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 307
- (Exam Topic 15)
An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.
Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

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

Answer: B

NEW QUESTION 308

- (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 310
- (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 311
- (Exam Topic 15)
In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

A. Wide focus
B. Strategic
C. Anticipate
D. Process

Answer: D

NEW QUESTION 315
- (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 318
- (Exam Topic 15)
What is the FIRST step in risk management?

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

Answer: C

NEW QUESTION 321
- (Exam Topic 15)
Which of the following is TRUE for an organization that is using a third-party federated identity service?

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

Answer: C

NEW QUESTION 324
- (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 329
- (Exam Topic 15)
An organization is implementing data encryption using symmetric ciphers and the Chief Information Officer (CIO) is concerned about the risk of using one key to protect all sensitive data, The security practitioner has been tasked with recommending a solution to address the CIO's concerns, Which of the following is the BEST approach to achieving the objective by encrypting all sensitive data?

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

Answer: D

NEW QUESTION 331
- (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 335
- (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 336
- (Exam Topic 15)
A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

A. Statically typed
B. Weakly typed
C. Strongly typed
D. Dynamically typed

Answer: D

NEW QUESTION 339
- (Exam Topic 15)
Which of the following attack types can be used to compromise the integrity of data during transmission?

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

Answer: B

NEW QUESTION 342
- (Exam Topic 15)
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

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

Answer: C

NEW QUESTION 345
- (Exam Topic 15)
A recent security audit is reporting several unsuccessful login attempts being repeated at specific times during the day on an Internet facing authentication server. No alerts have been generated by the security information and event management (SIEM) system. What PRIMARY action should be taken to improve SIEM performance?

A. Implement role-based system monitoring
B. Audit firewall logs to identify the source of login attempts
C. Enhance logging detail
D. Confirm alarm thresholds

Answer: B

NEW QUESTION 348
- (Exam Topic 15)
Which is the PRIMARY mechanism for providing the workforce with the information needed to protect an agency's vital information resources?

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

Answer: A

NEW QUESTION 351
- (Exam Topic 15)
The security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network. Which solution is MOST effective at discovering a successful network breach?

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

Answer: A

NEW QUESTION 355
- (Exam Topic 15)
A malicious user gains access to unprotected directories on a web server. Which of the following is MOST likely the cause for this information disclosure?

A. Security misconfiguration
B. Cross-site request forgery (CSRF)
C. Structured Query Language injection (SQLi)
D. Broken authentication management

Answer: A

NEW QUESTION 357
- (Exam Topic 15)
When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

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

Answer: B

NEW QUESTION 362
- (Exam Topic 15)
When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

A. Requirements
B. Risk assessment
C. Due diligence
D. Planning

Answer: B

NEW QUESTION 366
- (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 370

- (Exam Topic 15)
Which of the following statements BEST describes least privilege principle in a cloud environment?

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

Answer: B

NEW QUESTION 373
- (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 374
- (Exam Topic 15)
Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

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

Answer: A

NEW QUESTION 376
- (Exam Topic 15)
An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

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

Answer: B

NEW QUESTION 377
- (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 379
- (Exam Topic 15)
An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

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

Answer: A

NEW QUESTION 382
- (Exam Topic 15)
Which of the following BEST ensures the integrity of transactions to intended recipients?

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

Answer: A

NEW QUESTION 385
- (Exam Topic 15)
What are the first two components of logical access control?

A. Confidentiality and authentication
B. Authentication and identification
C. Identification and confidentiality
D. Authentication and availability

Answer: B

NEW QUESTION 389
- (Exam Topic 15)
Which of the following is the BEST option to reduce the network attack surface of a system?

A. Ensuring that there are no group accounts on the system
B. Removing unnecessary system user accounts
C. Disabling unnecessary ports and services
D. Uninstalling default software on the system

Answer: C

NEW QUESTION 394
- (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 396
- (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 399
- (Exam Topic 15)
When telephones in a city are connected by a single exchange, the caller can only connect with the switchboard operator. The operator then manually connects the call.
This is an example of which type of network topology?

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

Answer: A

NEW QUESTION 403
- (Exam Topic 15)
Secure coding can be developed by applying which one of the following?

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

Answer: B

NEW QUESTION 405

- (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 407
- (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 411
- (Exam Topic 15)
A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

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

Answer: C

NEW QUESTION 415
- (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 417
- (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 422
- (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 426
- (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 431
- (Exam Topic 15)
What is considered a compensating control for not having electrical surge protectors installed?

A. Having dual lines to network service providers built to the site
B. Having backup diesel generators installed to the site
C. Having a hot disaster recovery (DR) environment for the site
D. Having network equipment in active-active clusters at the site

Answer: D

NEW QUESTION 436
- (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 441
- (Exam Topic 15)
Which of the following security tools will ensure authorized data is sent to the application when implementing a cloud based application?

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

Answer: B

NEW QUESTION 445
- (Exam Topic 15)
All hosts on the network are sending logs via syslog-ng to the log collector. The log collector is behind its own firewall, The security professional wants to make sure not to put extra load on the firewall due to the amount of traffic that is passing through it. Which of the following types of filtering would MOST likely be used?

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

Answer: C

NEW QUESTION 446
- (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 448
- (Exam Topic 15)
A security engineer is required to integrate security into a software project that is implemented by small groups test quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process'

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

Answer: C

NEW QUESTION 450
- (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 452
- (Exam Topic 15)
Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

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

Answer: C

NEW QUESTION 453
- (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 456
- (Exam Topic 15)
What industry-recognized document could be used as a baseline reference that is related to data security and business operations for conducting a security assessment?

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

Answer: D

NEW QUESTION 460
- (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 462
- (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 467
- (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 471
- (Exam Topic 15)
employee training, risk management, and data handling procedures and policies could be characterized as which type of security measure?

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

Answer: D

NEW QUESTION 474
- (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 479
- (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 482
- (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 486
- (Exam Topic 15)
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

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

Answer: A

NEW QUESTION 490
- (Exam Topic 15)
Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

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

Answer: B

NEW QUESTION 492
- (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 495
- (Exam Topic 15)
What is the HIGHEST priority in agile development?

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

Answer: C

NEW QUESTION 499
- (Exam Topic 15)
The security architect has been mandated to assess the security of various brands of mobile devices. At what phase of the product lifecycle would this be MOST likely to occur?

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

Answer: C

NEW QUESTION 502
- (Exam Topic 15)
Which of the following contributes MOST to the effectiveness of a security officer?

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

Answer: A

NEW QUESTION 504
- (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 506
- (Exam Topic 15)
A company-wide penetration test result shows customers could access and read files through a web browser. Which of the following can be used to mitigate this vulnerability?

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

Answer: B

NEW QUESTION 510
- (Exam Topic 15)
In order to provide dual assurance in a digital signature system, the design MUST include which of the following?

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

Answer: B

NEW QUESTION 514
- (Exam Topic 15)
Which of the following is a covert channel type?

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

Answer: A

NEW QUESTION 519
- (Exam Topic 15)
Which of the following is a standard Access Control List (ACL) element that enables a router to filter Internet traffic?

A. Media Access Control (MAC) address
B. Internet Protocol (IP) address
C. Security roles
D. Device needs

Answer: B

NEW QUESTION 524
- (Exam Topic 15)
Which of the following activities should a forensic examiner perform FIRST when determining the priority of digital evidence collection at a crime scene?

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

Answer: C

NEW QUESTION 527
- (Exam Topic 15)
In which of the following scenarios is locking server cabinets and limiting access to keys preferable to locking the server room to prevent unauthorized access?

A. Server cabinets are located in an unshared workspace.
B. Server cabinets are located in an isolated server farm.
C. Server hardware is located in a remote area.
D. Server cabinets share workspace with multiple projects.

Answer: D

NEW QUESTION 529
- (Exam Topic 15)
When are security requirements the LEAST expensive to implement?

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

Answer: D

NEW QUESTION 531
- (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 534
- (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 537
- (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 542
- (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 543
- (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 544
- (Exam Topic 15)
Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

A. The business owner
B. security subject matter expert (SME)
C. The application owner
D. A developer subject matter expert (SME)

Answer: B

NEW QUESTION 546
- (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 551
- (Exam Topic 15)
Which of the fallowing statements is MOST accurate regarding information assets?

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

Answer: B

NEW QUESTION 555
- (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 558
- (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 563
- (Exam Topic 15)
Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

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

Answer: B

NEW QUESTION 566
- (Exam Topic 15)
A large organization’s human resources and security teams are planning on implementing technology to eliminate manual user access reviews and improve compliance. Which of the following options is MOST likely to resolve the issues associated with user access?

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

Answer: B

NEW QUESTION 567
- (Exam Topic 14)
Which of the following is the BEST technique to facilitate secure software development?

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

Answer: A

NEW QUESTION 570
- (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 572
- (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 576

- (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 580
- (Exam Topic 14)
What steps can be taken to prepare personally identifiable information (PII) for processing by a third party?

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

Answer: C

NEW QUESTION 581
- (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 583
- (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 587
- (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 589
- (Exam Topic 14)
Which of the following is TRUE regarding equivalence class testing?

A. It is characterized by the stateless behavior of a process implemented In a function.
B. An entire partition can be covered by considering only one representative value from that partition.
C. Test inputs are obtained from the derived boundaries of the given functional specifications.
D. It is useful for testing communications protocols and graphical user interfaces.

Answer: C

NEW QUESTION 590
- (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 591
- (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 592
- (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 596
- (Exam Topic 14)
Which of the following is the PRIMARY risk associated with Extensible Markup Language (XML) applications?

A. Users can manipulate the code.
B. The stack data structure cannot be replicated.
C. The stack data structure is repetitive.
D. Potential sensitive data leakage.

Answer: A

NEW QUESTION 600
- (Exam Topic 14)
For the purpose of classification, which of the following is used to divide trust domain and trust boundaries?

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

Answer: A

NEW QUESTION 605
- (Exam Topic 14)
If a content management system (CMC) is implemented, which one of the following would occur?

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

Answer: D

NEW QUESTION 607
- (Exam Topic 14)
Which of the following value comparisons MOST accurately reflects the agile development approach?

A. Processes and toots over individuals and interactions
B. Contract negotiation over customer collaboration
C. Following a plan over responding to change
D. Working software over comprehensive documentation

Answer: D

NEW QUESTION 612
- (Exam Topic 14)
Physical assets defined in an organization's Business Impact Analysis (BIA) could include which of the following?

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

Answer:

B

NEW QUESTION 616
- (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 617
- (Exam Topic 14)
Which of the following encryption types is used in Hash Message Authentication Code (HMAC) for key distribution?

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

Answer: A

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

NEW QUESTION 618
- (Exam Topic 14)
A corporate security policy specifies that all devices on the network must have updated operating system patches and anti-malware software. Which technology should be used to enforce this policy?

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

Answer: D

NEW QUESTION 623
- (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 628
- (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 630
- (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 633
- (Exam Topic 14)

Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

A. Process isolation
B. Data hiding and abstraction
C. Use of discrete layering and Application Programming Interfaces (API)
D. Virtual Private Network (VPN)

Answer: C

Explanation:
Reference: https://books.google.com.pk/books?id=LnjxBwAAQBAJ&pg=PT504&lpg=PT504&dq=CISSP+mechanism+us

NEW QUESTION 634
- (Exam Topic 14)
Which of the following four iterative steps are conducted on third-party vendors in an on-going basis?

A. Investigate, Evaluate, Respond, Monitor
B. Frame, Assess, Respond, Monitor
C. Frame, Assess, Remediate, Monitor
D. Investigate, Assess, Remediate, Monitor

Answer: C

NEW QUESTION 637
- (Exam Topic 14)
An organization has a short-term agreement with a public Cloud Service Provider (CSP). Which of the following BEST protects sensitive data once the agreement expires and the assets are reused?

A. Recommended that the business data owners use continuous monitoring and analysis of applications to prevent data loss.
B. Recommend that the business data owners use internal encryption keys for data-at-rest and data-in-transit to the storage environment.
C. Use a contractual agreement to ensure the CSP wipes the data from the storage environment.
D. Use a National Institute of Standards and Technology (NIST) recommendation for wiping data on the storage environment.

Answer: C

NEW QUESTION 640
- (Exam Topic 14)
What is the MOST common component of a vulnerability management framework?

A. Risk analysis
B. Patch management
C. Threat analysis
D. Backup management

Answer: B

Explanation:
Reference: https://www.helpnetsecurity.com/2016/10/11/effective-vulnerability-management-process/

NEW QUESTION 643
- (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 647
- (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 650
- (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 654
- (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 658
- (Exam Topic 14)
Which of the following is the final phase of the identity and access provisioning lifecycle?

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

Answer: B

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

NEW QUESTION 662
- (Exam Topic 14)
An organization discovers that its secure file transfer protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization's general information technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.
Which of the following is the MOST probable attack vector used in the security breach?

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

Answer: A

NEW QUESTION 665
- (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 666
- (Exam Topic 14)
Which layer of the Open system Interconnect (OSI) model is responsible for secure data transfer between applications, flow control, and error detection and correction?

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

Answer: B

NEW QUESTION 668
- (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 671
- (Exam Topic 14)
Which of the following is considered the last line defense in regard to a Governance, Risk managements, and compliance (GRC) program?

A. Internal audit
B. Internal controls
C. Board review
D. Risk management

Answer: B

NEW QUESTION 674
- (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 679
- (Exam Topic 14)
Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?

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

Answer: B

NEW QUESTION 684
- (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 687
- (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 692
- (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

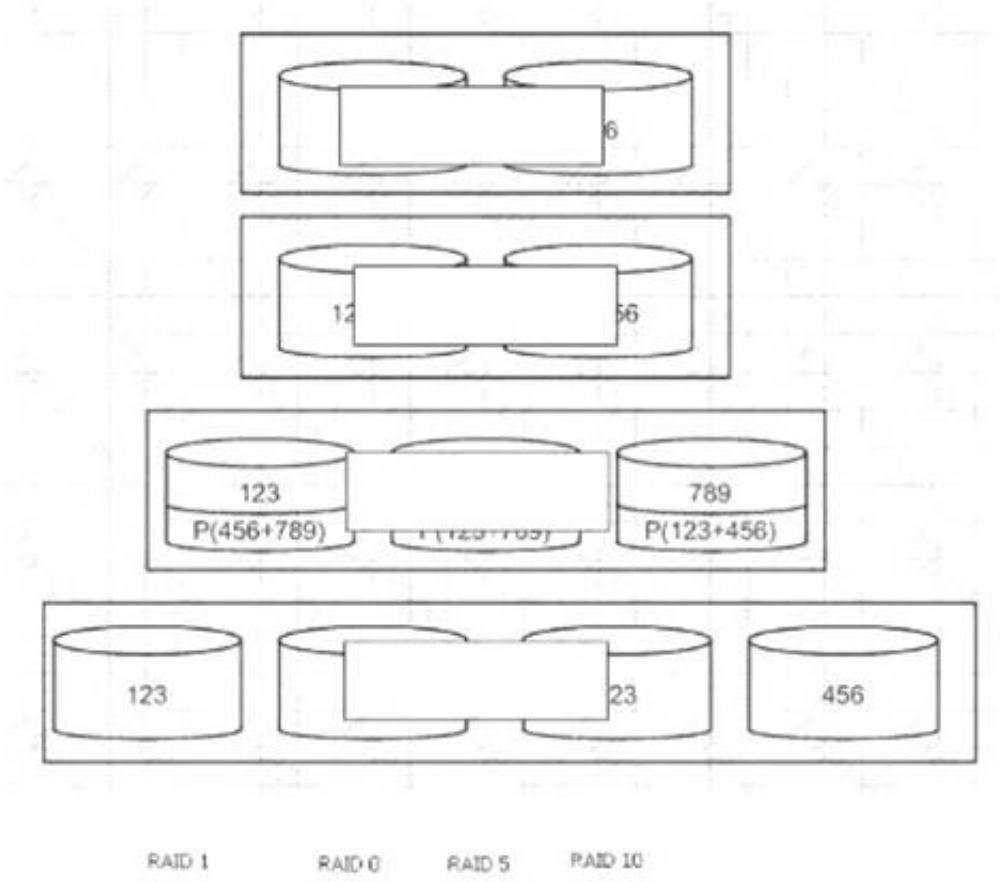
NEW QUESTION 696
- (Exam Topic 14)
Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

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

Answer: C

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

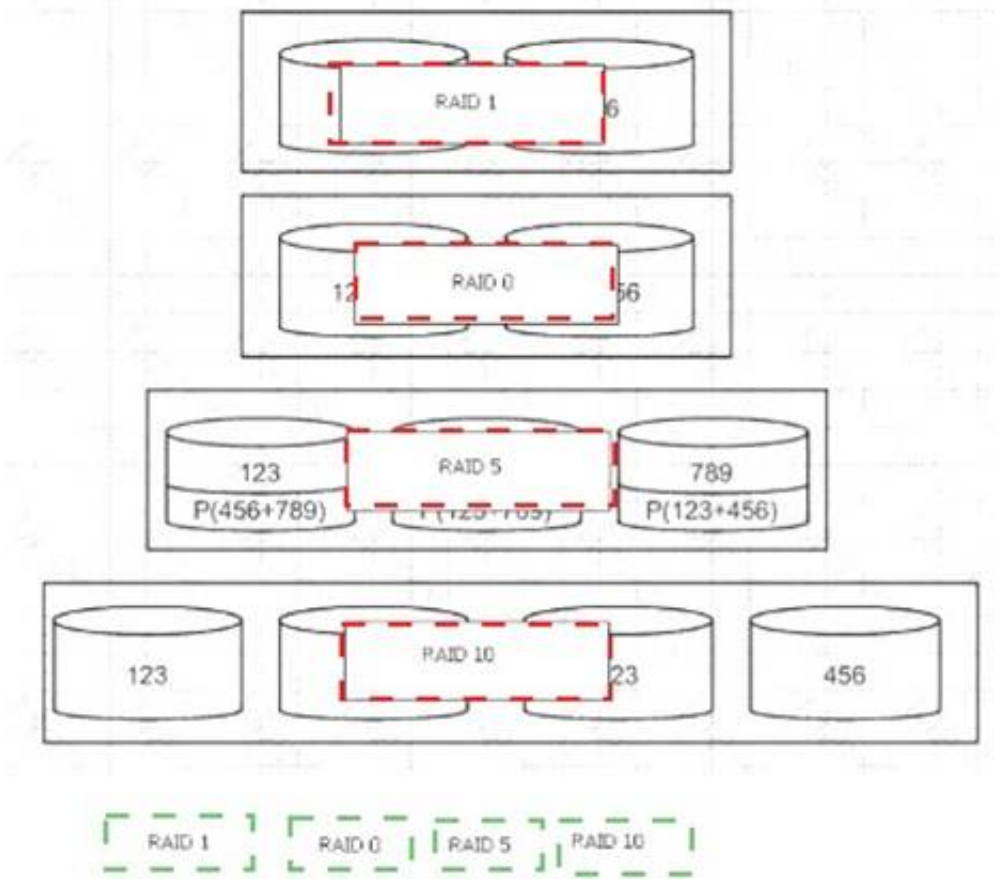
NEW QUESTION 699
- (Exam Topic 14)
Given a file containing ordered number, i.e. “123456789,” match each of the following redundant Array of independent Disks (RAID) levels to the corresponding visual representation visual representation. Note: P() = parity.
Drag each level to the appropriate place on the diagram.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 701
- (Exam Topic 14)
How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

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

Answer: A

NEW QUESTION 704
- (Exam Topic 14)
A new Chief Information Officer (CIO) created a group to write a data retention policy based on applicable laws. Which of the following is the PRIMARY motivation for the policy?

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

Answer: B

NEW QUESTION 707
- (Exam Topic 14)
Which of the following is a PRIMARY challenge when running a penetration test?

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

Answer: D

NEW QUESTION 709
- (Exam Topic 14)
The MAIN task of promoting security for Personal Computers (PC) is

A. understanding the technical controls and ensuring they are correctly installed.
B. understanding the required systems and patching processes for different Operating Systems (OS).
C. making sure that users are using only valid, authorized software, so that the chance of virus infection
D. making users understand the risks to the machines and data, so they will take appropriate steps to project them.

Answer: C

NEW QUESTION 710
- (Exam Topic 14)
What are the roles within a scrum methodoligy?

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

Answer: B

NEW QUESTION 713
- (Exam Topic 14)
Which of the following practices provides the development of security and identification of threats in designing software?

A. Stakeholder review
B. Requirements review
C. Penetration testing
D. Threat modeling

Answer: D

NEW QUESTION 715
- (Exam Topic 14)
Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device Which has stolen?

A. Whole device encryption with key escrow
B. Mobile Device Management (MDMJ with device wipe
C. Mobile device tracking with geolocation
D. Virtual Private Network (VPN) with traffic encryption

Answer: B

NEW QUESTION 717

- (Exam Topic 14)
Which is the second phase of public key Infrastructure (pk1) key/certificate life-cycle management?

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

Answer: C

NEW QUESTION 719
- (Exam Topic 14)
Which of the following phases involves researching a target's configuration from public sources when performing a penetration test?

A. Information gathering
B. Social engineering
C. Target selection
D. Traffic enumeration

Answer: A

NEW QUESTION 721
- (Exam Topic 14)
Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for implementing network security?

A. Peer authentication
B. Payload data encryption
C. Session encryption
D. Hashing digest

Answer: C

NEW QUESTION 726
- (Exam Topic 14)
What is the MAIN reason to ensure the appropriate retention periods are enforced for data stored on electronic media?

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

Answer: D

NEW QUESTION 731
- (Exam Topic 14)
Which is the MOST effective countermeasure to prevent electromagnetic emanations on unshielded data cable?

A. Move cable are away from exterior facing windows
B. Encase exposed cable runs in metal conduit
C. Enable Power over Ethernet (PoE) to increase voltage
D. Bundle exposed cables together to disguise their signals

Answer: B

NEW QUESTION 733
- (Exam Topic 14)
What is the FIRST step required in establishing a records retention program?

A. Identify and inventory all records storage locations.
B. Classify records based on sensitivity.
C. Identify and inventory all records.
D. Draft a records retention policy.

Answer: D

NEW QUESTION 737
- (Exam Topic 14)
Change management policies and procedures belong to which of the following types of controls?

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

Answer: A

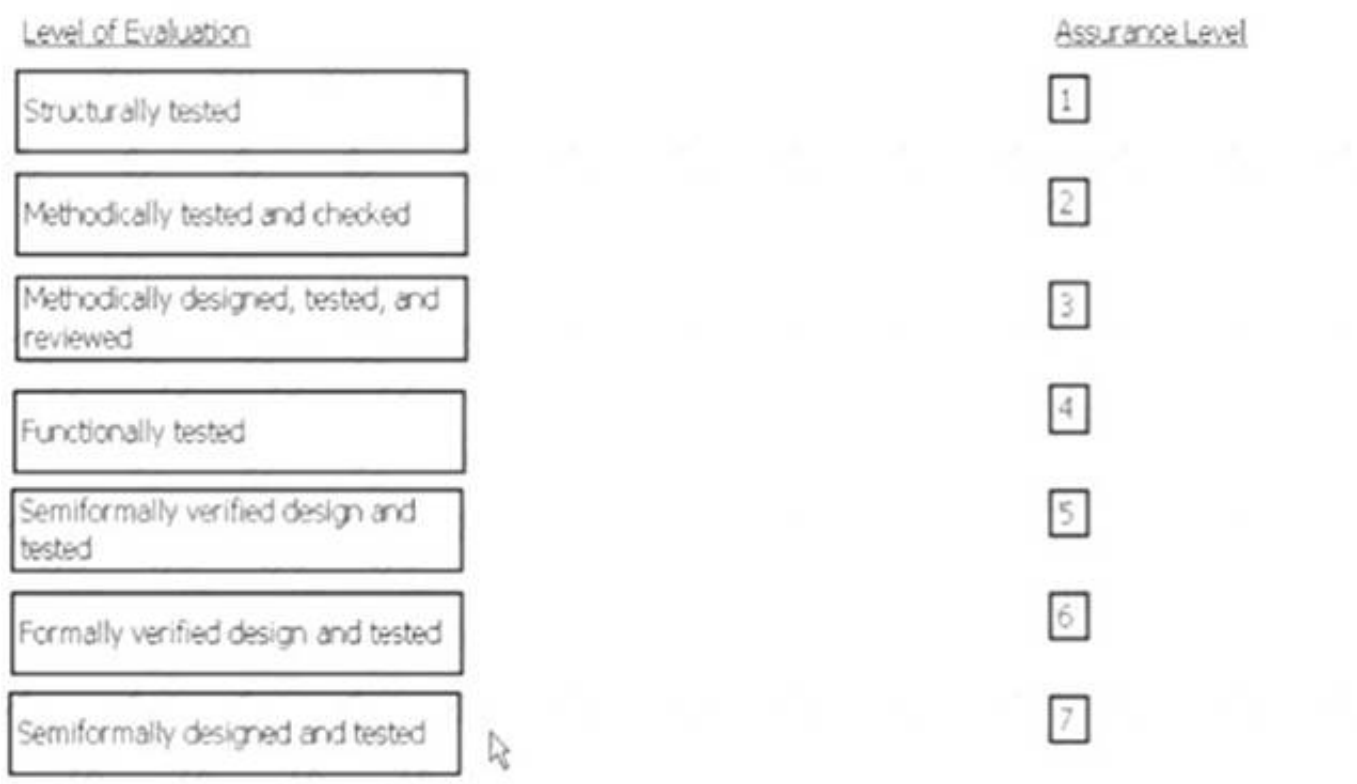
Explanation:
Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Change+mana

NEW QUESTION 741
- (Exam Topic 14)
Following a penetration test, what should an organization do FIRST?

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

Answer: D

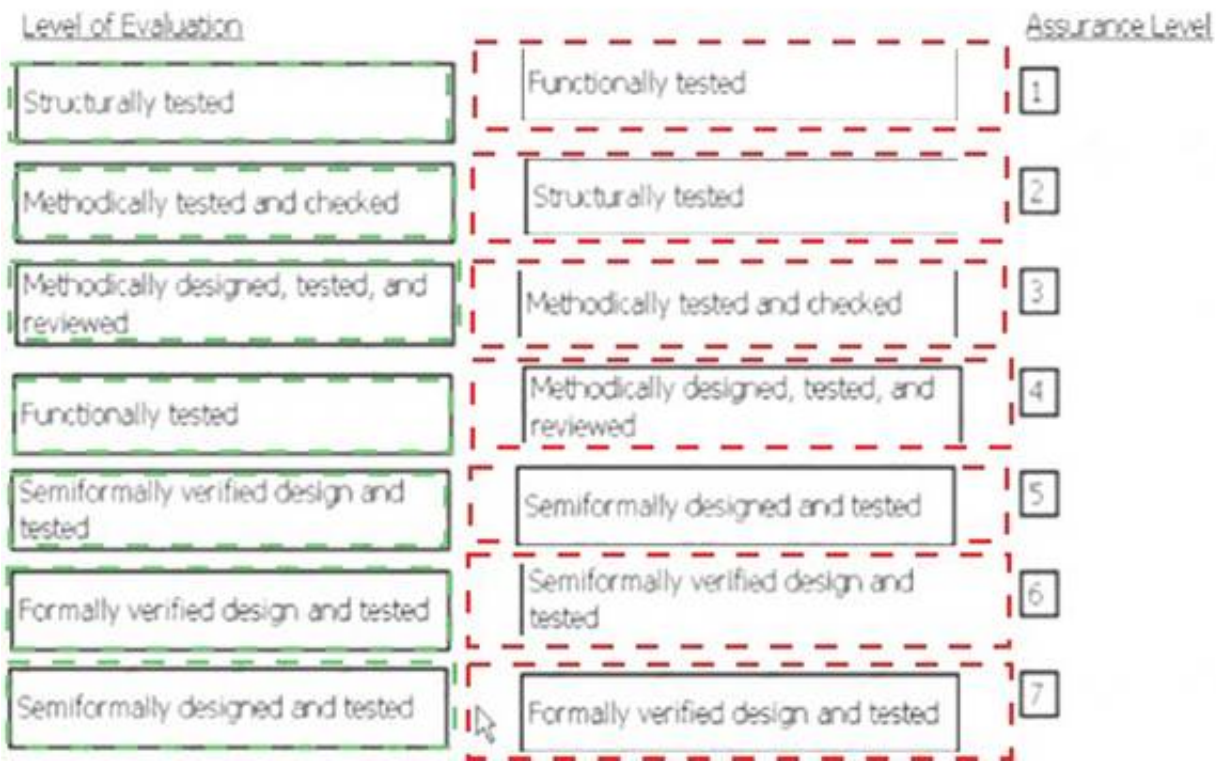
NEW QUESTION 745
- (Exam Topic 14)
Match the level of evaluation to the correct common criteria (CC) assurance level.
Drag each level of evaluation on the left to is corresponding CC assurance level on the right



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 746
- (Exam Topic 14)
Who is essential for developing effective test scenarios for disaster recovery (DR) test plans?

A. Business line management and IT staff members
B. Chief Information Officer (CIO) and DR manager

C. DR manager end IT staff members
D. IT staff members and project managers

Answer: B

NEW QUESTION 750
- (Exam Topic 14)
Which of the following steps should be conducted during the FIRST phase of software assurance in a generic acquisition process?

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

Answer: C

NEW QUESTION 751
- (Exam Topic 14)
Organization A is adding a large collection of confidential data records that it received when it acquired Organization B to its data store. Many of the users and staff from Organization B are no longer available. Which of the following MUST Organization A 0do to property classify and secure the acquired data?

A. Assign data owners from Organization A to the acquired data.
B. Create placeholder accounts that represent former users from Organization B.
C. Archive audit records that refer to users from Organization A.
D. Change the data classification for data acquired from Organization B.

Answer: A

NEW QUESTION 754
- (Exam Topic 14)
Which of the following is the MOST important action regarding authentication?

A. Granting access rights
B. Enrolling in the system
C. Establishing audit controls
D. Obtaining executive authorization

Answer: B

NEW QUESTION 756
- (Exam Topic 14)
Information security metrics provide the GREATEST value tp management when based upon the security manager’s knowledge of which of the following?

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

Answer: B

NEW QUESTION 758
- (Exam Topic 14)
Which of the following is PRIMARILY adopted for ensuring the integrity of information is preserved?

A. Data at rest protection
B. Transport Layer Security (TLS)
C. Role Based Access Control (RBAC)
D. One-way encryption

Answer: A

NEW QUESTION 762
- (Exam Topic 14)
A security professional recommends that a company integrate threat modeling into its Agile development processes. Which of the following BEST describes the benefits of this approach?

A. Reduce application development costs.
B. Potential threats are addressed later in the Software Development Life Cycle (SDLC).
C. Improve user acceptance of implemented security controls.
D. Potential threats are addressed earlier in the Software Development Life Cycle (SDLC).

Answer: D

NEW QUESTION 763
- (Exam Topic 14)

Which of the following is true of Service Organization Control (SOC) reports?

A. SOC 1 Type 2 reports assess the security, confidentiality, integrity, and availability of an organization's controls
B. SOC 2 Type 2 reports include information of interest to the service organization's management
C. SOC 2 Type 2 reports assess internal controls for financial reporting
D. SOC 3 Type 2 reports assess internal controls for financial reporting

Answer: B

Explanation:
Reference:
http://ssae16.businesscatalyst.com/SSAE16_reports.html

NEW QUESTION 765
- (Exam Topic 14)
When would an organization review a Business Continuity Management (BCM) system?

A. When major changes occur on systems
B. When personnel changes occur
C. Before and after Disaster Recovery (DR) tests
D. At planned intervals

Answer: D

NEW QUESTION 766
- (Exam Topic 14)
Which of the following MUST an organization do to effectively communicate is security strategy to all affected parties?

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

Answer: C

NEW QUESTION 769
- (Exam Topic 14)
Which of the following is MOST important when determining appropriate countermeasures for an identified risk?

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

Answer: C

NEW QUESTION 771
- (Exam Topic 14)
Which of the following will help prevent improper session handling?

A. Ensure that all UlWebView calls do not execute without proper input validation.
B. Ensure that tokens are sufficiently long, complex, and pseudo-random.
C. Ensure JavaScript and plugin support is disabled.
D. Ensure that certificates are valid and fail closed.

Answer: B

NEW QUESTION 775
- (Exam Topic 14)
A project requires the use of en authentication mechanism where playback must be protected and plaintext secret must be used. Which of the following should be used?

A. Password Authentication Protocol (PAP)
B. Extensible Authentication Protocol (EAP)
C. Secure Hash Algorithm (SHA)
D. Challenge Handshake Authentication Protocol (CHAP)

Answer: A

NEW QUESTION 776
- (Exam Topic 14)
Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

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

Answer: A

NEW QUESTION 778
- (Exam Topic 14)
Individual access to a network is BEST determined based on

A. risk matrix.
B. value of the data.
C. business need.
D. data classification.

Answer: C

NEW QUESTION 781
- (Exam Topic 14)
Which of the following should be included in a hardware retention policy? Which of the following should be included in a hardware retention policy?

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

Answer: A

NEW QUESTION 786
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

https://www.certleader.com/CISSP-dumps.html