ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

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

Answer: D

NEW QUESTION 2
- (Exam Topic 15)
An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

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

Answer: B

NEW QUESTION 3
- (Exam Topic 15)
In which process MUST security be considered during the acquisition of new software?

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

Answer: B

NEW QUESTION 4
- (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 5
- (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 6
- (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 7
- (Exam Topic 15)
he security organization is loading for a solution that could help them determine with a strong level of confident that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

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

Answer: B

NEW QUESTION 8
- (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 9
- (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 10
- (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 10
- (Exam Topic 15)
A breach investigation …… a website was exploited through an open soured …..Is The FIRB Stan In the Process that could have prevented this breach?

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

Answer: B

NEW QUESTION 11
- (Exam Topic 15)
An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP), The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract.
Which of the following MUST be included in the contract?

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

Answer: C

NEW QUESTION 15
- (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 19
- (Exam Topic 15)
When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

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

Answer: C

NEW QUESTION 22
- (Exam Topic 15)
When reviewing the security logs, the password shown for an administrative login event was ' OR ' '1'='1' --. This is an example of which of the following kinds of attack?

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

Answer: B

NEW QUESTION 23
- (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 25
- (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 30
- (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 34
- (Exam Topic 15)
Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

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

Answer: A

NEW QUESTION 37
- (Exam Topic 15)
In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to the resource’s access to the production operating system (OS) directory structure?

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

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

Answer: C

NEW QUESTION 38
- (Exam Topic 15)
During a Disaster Recovery (DR) simulation, it is discovered that the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans simultaneously. What would be impacted by this fact if left unchanged?

A. Recovery Point Objective (RPO)
B. Recovery Time Objective (RTO)
C. Business Impact Analysis (BIA)
D. Return on Investment (ROI)
E. A

Answer: E

NEW QUESTION 42
- (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 46
- (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 49
- (Exam Topic 15)
An organization recently upgraded to a Voice over Internet Protocol (VoIP) phone system. Management is concerned with unauthorized phone usage. Security consultant is responsible for putting together a plan to secure these phones. Administrators have assigned unique personal identification number codes for each person in the organization. What is the BEST solution?

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

Answer: C

NEW QUESTION 53
- (Exam Topic 15)
Which of the following statements BEST distinguishes a stateful packet inspection firewall from a stateless packet filter firewall?

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

Answer: B

NEW QUESTION 57
- (Exam Topic 15)
What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

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

Answer: B

NEW QUESTION 62
- (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 66
- (Exam Topic 15)
Why is data classification control important to an organization?

A. To ensure its integrity, confidentiality and availability
B. To enable data discovery
C. To control data retention in alignment with organizational policies and regulation
D. To ensure security controls align with organizational risk appetite

Answer: A

NEW QUESTION 70
- (Exam Topic 15)
Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

A. All sources are reporting in the exact same Extensible Markup Language (XML) format.
B. Data sources do not contain information infringing upon privacy regulations.
C. All sources are synchronized with a common time reference.
D. Each source uses the same Internet Protocol (IP) address for reporting.

Answer: C

NEW QUESTION 72
- (Exam Topic 15)
A project manager for a large software firm has acquired a government contract that generates large amounts of Controlled Unclassified Information (CUI). The organization's information security manager has received a request to transfer project-related CUI between systems of differing security classifications. What role provides
the authoritative guidance for this transfer?

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

Answer: C

NEW QUESTION 77
- (Exam Topic 15)
A digitally-signed e-mail was delivered over a wireless network protected with Wired Equivalent Privacy (WEP) protocol. Which of the following principles is at risk?

A. Availability
B. Non-Repudiation
C. Confidentiality
D. Integrity

Answer: B

NEW QUESTION 79
- (Exam Topic 15)
Which of the following is the BEST way to mitigate circumvention of access controls?

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

Answer: D

NEW QUESTION 80
- (Exam Topic 15)
Which of the following regulations dictates how data breaches are handled?

A. Sarbanes-Oxley (SOX)
B. National Institute of Standards and Technology (NIST)

C. Payment Card Industry Data Security Standard (PCI-DSS)
D. General Data Protection Regulation (GDPR)

Answer: D

NEW QUESTION 84
- (Exam Topic 15)
Which of the following BEST describes the objectives of the Business Impact Analysis (BIA)?

A. Identifying the events and environmental factors that can adversely affect an organization
B. Identifying what is important and critical based on disruptions that can affect the organization.
C. Establishing the need for a Business Continuity Plan (BCP) based on threats that can affect an organization
D. Preparing a program to create an organizational awareness for executing the Business Continuity Plan (BCP)

Answer: B

NEW QUESTION 89
- (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 90
- (Exam Topic 15)
Which of the following examples is BEST to minimize the attack surface for a customer's private information?

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

Answer: A

NEW QUESTION 94
- (Exam Topic 15)
Which of the following is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions?

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

Answer: D

NEW QUESTION 97
- (Exam Topic 15)
A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

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

Answer: D

NEW QUESTION 101
- (Exam Topic 15)
As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem?

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

Answer: C

NEW QUESTION 102
- (Exam Topic 15)

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

Answer: D

NEW QUESTION 105
- (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 108
- (Exam Topic 15)
An establish information technology (IT) consulting firm is considering acquiring a successful local startup. To gain a comprehensive understanding of the startup's security posture' which type of assessment provides the BEST information?

A. A security audit
B. A penetration test
C. A tabletop exercise
D. A security threat model

Answer: A

NEW QUESTION 112
- (Exam Topic 15)
Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

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

Answer: B

NEW QUESTION 114
- (Exam Topic 15)
A financial services organization has employed a security consultant to review processes used by employees across various teams. The consultant interviewed a member of the application development practice and found gaps in their threat model. Which of the following correctly represents a trigger for when a threat model should be revised?

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

Answer: D

NEW QUESTION 116
- (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 services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

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

Answer: A

NEW QUESTION 121
- (Exam Topic 15)
What is the term used to define where data is geographically stored in the cloud?

A. Data warehouse
B. Data privacy rights
C. Data subject rights
D. Data sovereignty

Answer: D

NEW QUESTION 126
- (Exam Topic 15)
A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

A. Omni
B. Directional
C. Yagi
D. Parabolic

Answer: A

NEW QUESTION 127
- (Exam Topic 15)
Which of the following is included in change management?

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

Answer: A

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

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

Answer: C

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

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

Answer: C

NEW QUESTION 137
- (Exam Topic 15)
In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below.
Which of the following would be a reasonable annual loss expectation?

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

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

Answer: B

NEW QUESTION 139
- (Exam Topic 15)
When testing password strength, which of the following is the BEST method for brute forcing passwords?

A. Conduct an offline attack on the hashed password information.
B. Conduct an online password attack until the account being used is locked.
C. Use a comprehensive list of words to attempt to guess the password.
D. Use social engineering methods to attempt to obtain the password.

Answer: C

NEW QUESTION 142
- (Exam Topic 15)
A developer begins employment with an information technology (IT) organization. On the first day, the developer works through the list of assigned projects and finds that some files within those projects aren't accessible, Other developers working on the same project have no trouble locating and working on the. What is the MOST likely explanation for the discrepancy in access?

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

Answer: A

NEW QUESTION 144
- (Exam Topic 15)
What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

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

Answer: A

NEW QUESTION 146
- (Exam Topic 15)
Which of the following is an open standard for exchanging authentication and authorization data between parties?

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

Answer: D

NEW QUESTION 149
- (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 150
- (Exam Topic 15)
Which of the following criteria ensures information is protected relative to its importance to the organization?

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

Answer: D

NEW QUESTION 151
- (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 152
- (Exam Topic 15)
What security principle addresses the issue of "Security by Obscurity"?

A. Open design
B. Segregation of duties (SoD)
C. Role Based Access Control (RBAC)
D. Least privilege

Answer: D

NEW QUESTION 154
- (Exam Topic 15)
A security professional should ensure that clients support which secondary algorithm for digital signatures when a Secure Multipurpose Internet Mail Extension (S/MIME) is used?

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

Answer: C

NEW QUESTION 155
- (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 157
- (Exam Topic 15)
Computer forensics requires which of the following MAIN steps?

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

Answer: B

NEW QUESTION 160
- (Exam Topic 15)
Which of the following is the MOST appropriate control for asset data labeling procedures?

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

Answer: C

NEW QUESTION 163
- (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 165
- (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 166
- (Exam Topic 15)
Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

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

Answer: C

NEW QUESTION 171
- (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 176
- (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 179
- (Exam Topic 15)
What is the MOST important goal of conducting security assessments?

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

Answer: B

NEW QUESTION 182
- (Exam Topic 15)
A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

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

Answer: D

NEW QUESTION 184
- (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 187
- (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 190
- (Exam Topic 15)
Which of the following is the reason that transposition ciphers are easily recognizable?

A. Key
B. Block
C. Stream
D. Character

Answer: B

NEW QUESTION 192
- (Exam Topic 15)
Which of the following is the PRIMARY issue when analyzing detailed log information?

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

Answer: D

NEW QUESTION 193
- (Exam Topic 15)
Which of the following describes the order in which a digital forensic process is usually conducted?

A. Ascertain legal authority, agree upon examination strategy, conduct examination, and report results
B. Ascertain legal authority, conduct investigation, report results, and agree upon examination strategy
C. Agree upon examination strategy, ascertain legal authority, conduct examination, and report results
D. Agree upon examination strategy, ascertain legal authority, report results, and conduct examination

Answer: A

NEW QUESTION 194
- (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 195
- (Exam Topic 15)
Which of the following addresses requirements of security assessments during software acquisition?

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

Answer: A

NEW QUESTION 196
- (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 197
- (Exam Topic 15)
Which of the following will an organization's network vulnerability testing process BEST enhance?

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

Answer: C

NEW QUESTION 202
- (Exam Topic 15)
What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

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

Answer: C

NEW QUESTION 206
- (Exam Topic 15)
Data remanence is the biggest threat in which of the following scenarios?

A. A physical disk drive has been overwritten and reused within a datacenter.
B. A physical disk drive has been degaussed, verified, and released to a third party for dest…….
C. A flash drive has been overwritten, verified, and reused within a datacenter.
D. A flash drive has been overwritten and released to a third party for destruction.

Answer: D

NEW QUESTION 211
- (Exam Topic 15)
Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

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

Answer: B

NEW QUESTION 216
- (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 221
- (Exam Topic 15)
Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

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

Answer: B

NEW QUESTION 222
- (Exam Topic 15)
Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

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

Answer: B

NEW QUESTION 225
- (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 226
- (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 228
- (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 231
- (Exam Topic 15)
Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

A. RJ11
B. LC ports
C. Patch panel
D. F-type connector

Answer: C

NEW QUESTION 234
- (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 236
- (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 241
- (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 245
- (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 246
- (Exam Topic 15)
A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

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

Answer: B

NEW QUESTION 249
- (Exam Topic 15)
Which of the following BEST obtains an objective audit of security controls?

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

Answer: A

NEW QUESTION 252
- (Exam Topic 15)
The security team has been tasked with performing an interface test against a frontend external facing application and needs to verify that all input fields protect against
invalid input. Which of the following BEST assists this process?

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

Answer: A

NEW QUESTION 256
- (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 260
- (Exam Topic 15)
Which of the following is a unique feature of attribute-based access control (ABAC)?

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

Answer: C

NEW QUESTION 263
- (Exam Topic 15)
Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

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

Answer: A

NEW QUESTION 266
- (Exam Topic 15)
Which of the following BEST describes why software assurance is critical in helping prevent an increase in business and mission risk for an organization?

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

Answer: B

NEW QUESTION 269
- (Exam Topic 15)
What is the MOST important factor in establishing an effective Information Security Awareness Program?

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

Answer: C

NEW QUESTION 270
- (Exam Topic 15)
A new site's gateway isn't able to form a tunnel to the existing site-to-site Internet Protocol Security (IPsec) virtual private network (VPN) device at headquarters. Devices at the new site have no problem accessing resources on the Internet. When testing connectivity between the remote site’s gateway, it was observed that the external Internet Protocol (IP) address of the gateway was set to 192.168.1.1. and was configured to send outbound traffic to the Internet Service Provider (ISP) gateway at4 192.168.1.2. Which of the following would be the BEST way to resolve the issue and get the remote site connected?

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

Answer: A

NEW QUESTION 271
- (Exam Topic 15)
At what stage of the Software Development Life Cycle (SDLC) does software vulnerability remediation MOST likely cost the least to implement?

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

Answer: D

NEW QUESTION 275
- (Exam Topic 15)
Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

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

Answer: A

NEW QUESTION 277
- (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 278
- (Exam Topic 15)
The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the focresight to enable what feature on all endpoints?

A. Process isolation
B. Trusted Platform Module (TPM)
C. Address Space Layout Randomization (ASLR)
D. Virtualization

Answer: C

NEW QUESTION 283
- (Exam Topic 15)
During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

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

Answer: B

NEW QUESTION 287
- (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 291
- (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 295
- (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 300
- (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 305
- (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 310
- (Exam Topic 15)
Which of the following is the MOST effective measure for dealing with rootkit attacks?

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

Answer: D

NEW QUESTION 315
- (Exam Topic 15)
A software development company found odd behavior in some recently developed software, creating a need for a more thorough code review. What is the MOST effective argument for a more thorough code review?

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

Answer: D

NEW QUESTION 316
- (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 321
- (Exam Topic 15)
Digital non-repudiation requires which of the following?

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

Answer: A

NEW QUESTION 322
- (Exam Topic 15)
Which of the following is the PRIMARY type of cryptography required to support non-repudiation of a digitally signed document?

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

Answer: A

NEW QUESTION 324

- (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 325
- (Exam Topic 15)
Which of the following encryption technologies has the ability to function as a stream cipher?

A. Cipher Feedback (CFB)
B. Feistel cipher
C. Cipher Block Chaining (CBC) with error propagation
D. Electronic Code Book (ECB)

Answer: A

NEW QUESTION 328
- (Exam Topic 15)
Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

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

Answer: A

NEW QUESTION 331
- (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 332
- (Exam Topic 15)
Of the following, which BEST provides non- repudiation with regards to access to a server room?

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

Answer: C

NEW QUESTION 334
- (Exam Topic 15)
When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

A. The actual origin and tools used for the test can be hidden.
B. Information may be found on related breaches and hacking.
C. Vulnerabilities can be tested without impact on the tested environment.
D. Information may be found on hidden vendor patches.

Answer: D

NEW QUESTION 335
- (Exam Topic 15)
A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

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

Answer: D

NEW QUESTION 337
- (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 339
- (Exam Topic 15)
What is the PRIMARY objective of business continuity planning?

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

Answer: B

NEW QUESTION 344
- (Exam Topic 15)
Before allowing a web application into the production environment, the security practitioner performs multiple types of tests to confirm that the web application performs as expected. To test the username field, the security practitioner creates a test that enters more characters into the field than is allowed. Which of the following BEST describes the type of test performed?

A. Misuse case testing
B. Penetration testing
C. Web session testing
D. Interface testing

Answer: A

NEW QUESTION 347
- (Exam Topic 15)
An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 1
B. 2
C. 3

Answer: A

NEW QUESTION 348
- (Exam Topic 15)
Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

A. lntegrity
B. Scalability
C. Availability
D. Confidentiality

Answer: A

NEW QUESTION 350
- (Exam Topic 15)
What is the BEST method to use for assessing the security impact of acquired software?

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

Answer: B

NEW QUESTION 352
- (Exam Topic 15)
Which of the following BEST describes the standard used to exchange authorization information between different identity management systems?

A. Security Assertion Markup Language (SAML)

B. Service Oriented Architecture (SOA)
C. Extensible Markup Language (XML)
D. Wireless Authentication Protocol (WAP)

Answer: A

NEW QUESTION 353
- (Exam Topic 15)
What is the MOST common security risk of a mobile device?

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

Answer: C

NEW QUESTION 356
- (Exam Topic 15)
What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

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

Answer: C

NEW QUESTION 360
- (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 362
- (Exam Topic 15)
What is the second phase of public key infrastructure (PKI) key/certificate life-cycle management?

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

Answer: A

NEW QUESTION 363
- (Exam Topic 15)
Which of the following vulnerabilities can be BEST detected using automated analysis?

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

Answer: D

NEW QUESTION 366
- (Exam Topic 15)
International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

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

Answer: C

NEW QUESTION 367
- (Exam Topic 15)

A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

A. Intrusion prevention system (IPS)
B. Multi-factor authentication (MFA)
C. Data loss protection (DLP)
D. Data at rest encryption

Answer: B

NEW QUESTION 370
- (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 373
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

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

Answer: C

NEW QUESTION 375
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

Answer: B

NEW QUESTION 376
- (Exam Topic 15)
In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

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

Answer: A

NEW QUESTION 381
- (Exam Topic 15)
A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory risk to the company. The manager MOST likely discovered this during which of the following?

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

Answer: B

NEW QUESTION 382
- (Exam Topic 15)
A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

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

Answer: C

NEW QUESTION 384
- (Exam Topic 15)
Which of the following technologies can be used to monitor and dynamically respond to potential threats on web applications?

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

Answer: C

NEW QUESTION 388
- (Exam Topic 15)
Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

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

Answer: A

NEW QUESTION 393
- (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 398
- (Exam Topic 15)
Which type of access control includes a system that allows only users that are type=managers and department=sales to access employee records?

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

Answer: C

NEW QUESTION 399
- (Exam Topic 15)
Why are packet filtering routers used in low-risk environments?

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

Answer: B

NEW QUESTION 400
- (Exam Topic 15)
A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging generates extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

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

Answer: D

NEW QUESTION 403
- (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 406
- (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 410
- (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 411
- (Exam Topic 15)
Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

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

Answer: A

NEW QUESTION 415
- (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 419
- (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 420
- (Exam Topic 15)
What is the FIRST step prior to executing a test of an organisation's disaster recovery (DR) or business continuity plan (BCP)?

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

Answer: D

NEW QUESTION 424

- (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 428
- (Exam Topic 15)
A company needs to provide employee access to travel services, which are hosted by a third-party service provider, Employee experience is important, and when users are already authenticated, access to the travel portal is seamless. Which of the following methods is used to share information and grant user access to the travel portal?

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

Answer: D

NEW QUESTION 432
- (Exam Topic 15)
Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages?

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

Answer: C

NEW QUESTION 434
- (Exam Topic 15)
Which of the following is the MOST secure protocol for zremote command access to the firewall?

A. Secure Shell (SSH)
B. Trivial File Transfer Protocol (TFTP)
C. Hypertext Transfer Protocol Secure (HTTPS)
D. Simple Network Management Protocol (SNMP) v1

Answer: A

NEW QUESTION 436
- (Exam Topic 15)
When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner’s first consideration?

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

Answer: A

NEW QUESTION 437
- (Exam Topic 15)
A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

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

Answer: C

NEW QUESTION 440
- (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 444
- (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 445
- (Exam Topic 15)
Which media sanitization methods should be used for data with a high security categorization?

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

Answer: D

NEW QUESTION 448
- (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 450
- (Exam Topic 15)
Which of the following is the MOST effective corrective control to minimize the effects of a physical intrusion?

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

Answer: C

NEW QUESTION 455
- (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 456
- (Exam Topic 15)
During testing, where are the requirements to inform parent organizations, law enforcement, and a computer incident response team documented?

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

Answer: D

NEW QUESTION 460

- (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 463
- (Exam Topic 15)
Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?\

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

Answer: C

NEW QUESTION 465
- (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 468
- (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 469
- (Exam Topic 15)
What type of risk is related to the sequences of value-adding and managerial activities undertaken in an organization?

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

Answer: B

NEW QUESTION 470
- (Exam Topic 15)
In an environment where there is not full administrative control over all network connected endpoints, such as a university where non-corporate devices are used, what is
the BEST way to restrict access to the network?

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

Answer: A

NEW QUESTION 472
- (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 477
- (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 479
- (Exam Topic 15)
Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

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

Answer: C

NEW QUESTION 484
- (Exam Topic 15)
A hospital's building controls system monitors and operates the environmental equipment to maintain a safe and comfortable environment. Which of the following could be
used to minimize the risk of utility supply interruption?

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

Answer: D

NEW QUESTION 486
- (Exam Topic 15)
What is the MOST common cause of Remote Desktop Protocol (RDP) compromise?

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

Answer: B

NEW QUESTION 490
- (Exam Topic 15)
In Federated Identity Management (FIM), which of the following represents the concept of federation?

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

Answer: D

NEW QUESTION 493
- (Exam Topic 15)
Which of the following is a risk matrix?

A. A database of risks associated with a specific information system.
B. A table of risk management factors for management to consider.
C. A two-dimensional picture of risk for organizations, products, projects, or other items of interest.
D. A tool for determining risk management decisions for an activity or system.

Answer: C

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

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

Answer: A

NEW QUESTION 502
- (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 504
- (Exam Topic 15)
When MUST an organization's information security strategic plan be reviewed?

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

Answer: D

NEW QUESTION 507
- (Exam Topic 15)
Which of the following is the MOST effective strategy to prevent an attacker from disabling a network?

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

Answer: D

NEW QUESTION 508
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

Answer: C

NEW QUESTION 511
- (Exam Topic 15)
What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

A. Familiar syntax, abstraction of network topology, and definition of network protocols
B. Network syntax, abstraction of network flow, and abstraction of network protocols
C. Network syntax, abstraction of network commands, and abstraction of network protocols
D. Familiar syntax, abstraction of network topology, and abstraction of network protocols

Answer: C

NEW QUESTION 513
- (Exam Topic 15)
Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

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

Answer: A

NEW QUESTION 517
- (Exam Topic 15)
A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several 'open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

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

Answer: C

NEW QUESTION 521
- (Exam Topic 15)
An internal audit for an organization recently identified malicious actions by a user account. Upon further investigation, it was determined the offending user account was used by multiple people at multiple locations simultaneously for various services and applications. What is the BEST method to prevent this problem in the future?

A. Ensure the security information and event management (SIEM) is set to alert.
B. Inform users only one user should be using the account at a time.
C. Ensure each user has their own unique account,
D. Allow several users to share a generic account.

Answer: A

NEW QUESTION 525
- (Exam Topic 15)
What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

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

Answer: D

NEW QUESTION 527
- (Exam Topic 15)
Which of the following are all elements of a disaster recovery plan (DRP)?

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

Answer: C

NEW QUESTION 528
- (Exam Topic 15)
What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

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

Answer: D

NEW QUESTION 532
- (Exam Topic 15)
Which of the following is the MAIN benefit of off-site storage?

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

Answer: A

NEW QUESTION 534
- (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 535
- (Exam Topic 14)
What is the MOST effective way to determine a mission critical asset in an organization?

A. Vulnerability analysis
B. business process analysis
C. Threat analysis
D. Business risk analysis

Answer: B

NEW QUESTION 537
- (Exam Topic 14)
In a dispersed network that lacks central control, which of the following is die PRIMARY course of action to mitigate exposure?

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

Answer: C

NEW QUESTION 541
- (Exam Topic 14)
Which of the following is used to support the concept of defense in depth during the development phase of a software product?

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

Answer: B

NEW QUESTION 546
- (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 549
- (Exam Topic 14)
An organization wants to enable uses to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (F1M). Which of the following is used behind the scenes in a FIM deployment?

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

Answer: C

NEW QUESTION 554
- (Exam Topic 14)
copyright provides protection for which of the following?

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

Answer: C

NEW QUESTION 555
- (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 559
- (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 561
- (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 562
- (Exam Topic 14)
How long should the records on a project be retained?

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

Answer: B

NEW QUESTION 564
- (Exam Topic 14)
What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

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

Answer: D

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

NEW QUESTION 566
- (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 571
- (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 573
- (Exam Topic 14)
The Secure Shell (SSH) version 2 protocol supports.

A. availability, accountability, compression, and integrity,
B. authentication, availability, confidentiality, and integrity.
C. accountability, compression, confidentiality, and integrity.
D. authentication, compression, confidentiality, and integrity.

Answer: D

NEW QUESTION 577
- (Exam Topic 14)
Which of the following is the GREATEST security risk associated with the user of identity as a service (IDaaS) when an organization its own software?

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

Answer: B

NEW QUESTION 578
- (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 581
- (Exam Topic 14)
When adopting software as a service (Saas), which security responsibility will remain with remain with the adopting organization?

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

Answer: B

NEW QUESTION 586
- (Exam Topic 14)
A security practitioner has been tasked with establishing organizational asset handling procedures. What should be considered that would have the GRFATEST impact to the development of these procedures?

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

Answer: D

NEW QUESTION 591
- (Exam Topic 14)
Which is the MOST critical aspect of computer-generated evidence?

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

Answer: B

NEW QUESTION 596
- (Exam Topic 14)
Which of the following is a characteristic of convert security testing?

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

Answer: B

NEW QUESTION 600
- (Exam Topic 14)
Which of the following is the MOST important reason for using a chain of custody from?

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

Answer: A

NEW QUESTION 602
- (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 605
- (Exam Topic 14)
What is the PRIMARY purpose for an organization to conduct a security audit?

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

Answer: A

NEW QUESTION 609
- (Exam Topic 14)
Which of the following is used to detect steganography?

A. Audio analysis
B. Statistical analysis
C. Reverse engineering
D. Cryptanalysis

Answer: C

NEW QUESTION 614
- (Exam Topic 14)
Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

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

Answer: A

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

NEW QUESTION 616
- (Exam Topic 14)
When dealing with shared, privilaged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

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

Answer: B

NEW QUESTION 618
- (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 621
- (Exam Topic 14)
Which is the RECOMMENDED configuration mode for sensors for an intrusion prevention system (IPS) if the prevention capabilities will be used?

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

Answer: C

NEW QUESTION 623
- (Exam Topic 14)
During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should en assessor do?

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

Answer: A

NEW QUESTION 626
- (Exam Topic 14)
Which of the following is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services?

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

Answer: C

NEW QUESTION 627
- (Exam Topic 14)
Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

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

Answer: B

NEW QUESTION 631
- (Exam Topic 14)
Which of the following is the MOST critical success factor in the security patch management process?

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

Answer: A

NEW QUESTION 636
- (Exam Topic 14)
From an asset security perspective, what is the BEST countermeasure to prevent data theft due to data remanence when a sensitive data storage media is no longer needed?

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

Answer: C

NEW QUESTION 639
- (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 641
- (Exam Topic 14)
An organization that has achieved a Capability Maturity model Integration (CMMI) level of 4 has done which of the following?

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

Answer: C

NEW QUESTION 645
- (Exam Topic 14)
Who determines the required level of independence for security control Assessors (SCA)?

A. Business owner
B. Authorizing Official (AO)
C. Chief Information Security Officer (CISC)
D. System owner

Answer: B

NEW QUESTION 647
- (Exam Topic 14)
In order for application developers to detect potential vulnerabilities earlier during the Software Development Life Cycle (SDLC), which of the following safeguards should be implemented FIRST as part of a comprehensive testing framework?

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

Answer: A

NEW QUESTION 651
- (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 655
- (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 658
- (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 659
- (Exam Topic 14)
Which of the following is the BEST statement for a professional to include as port of business continuity (BC) procedure?

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

Answer: D

NEW QUESTION 660
- (Exam Topic 14)
An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.
Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

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

Answer: A

NEW QUESTION 662
- (Exam Topic 14)
Which open standard could l large corporation deploy for authorization services for single sign-on (SSO) use across multiple internal and external application?

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

Answer: B

NEW QUESTION 663
- (Exam Topic 14)
Which of the following BEST describes how access to a system is granted to federated user accounts?

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

Answer: C

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

NEW QUESTION 666
- (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 667
- (Exam Topic 14)
Which layer of the Open systems Interconnection (OSI) model is being targeted in the event of a Synchronization (SYN) flood attack?

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

Answer:

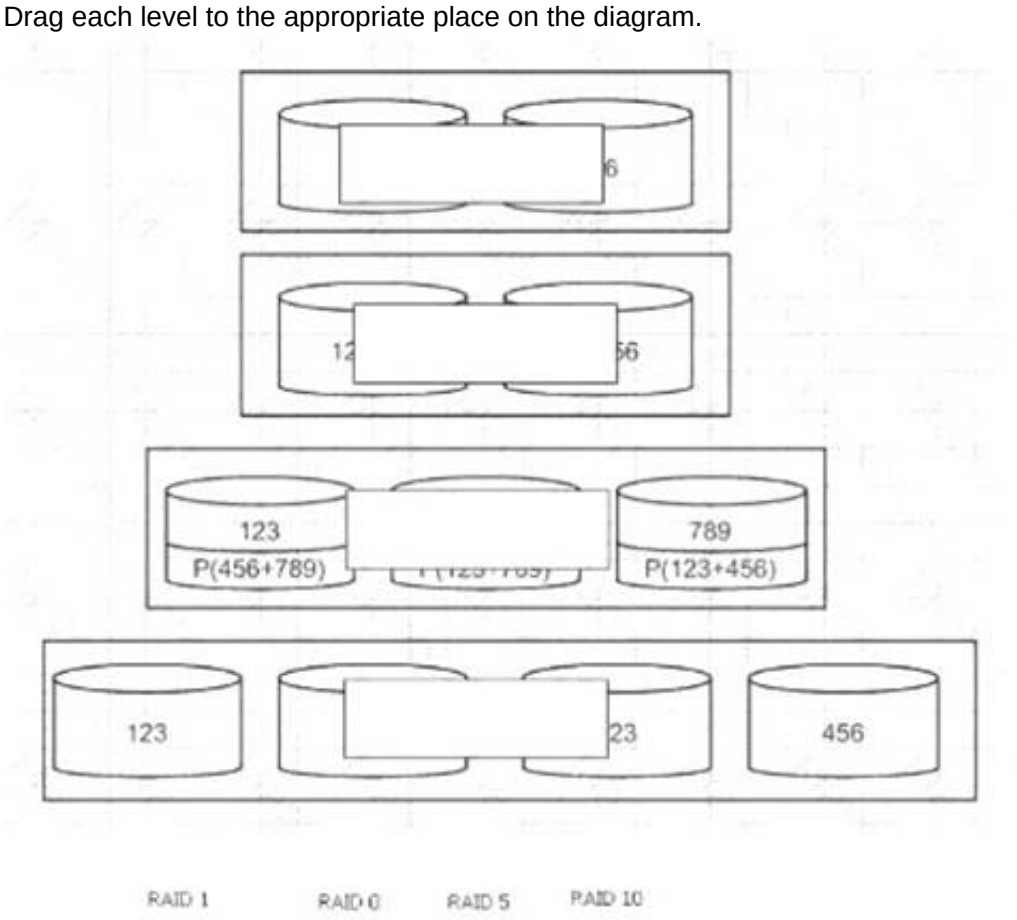
B

NEW QUESTION 671
- (Exam Topic 14)
What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

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

Answer: C

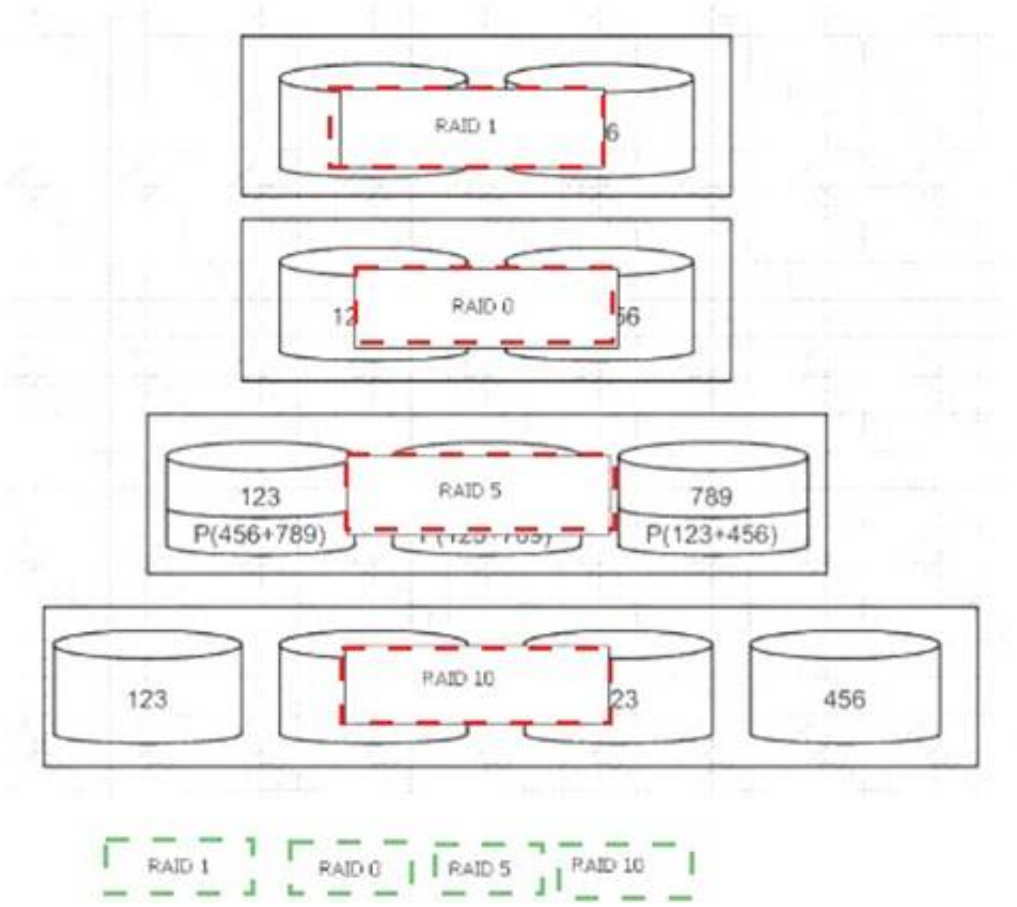
NEW QUESTION 676
- (Exam Topic 14)
Given a file containing ordered number, i.e. “123456789,” match each of the following redundant Array of independent Disks (RAID) levels to the corresponding visual representation visual representation. Note: P() = parity.
Drag each level to the appropriate place on the diagram.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 680
- (Exam Topic 14)
A security architect is responsible for the protection of a new home banking system. Which of the following solutions can BEST improve the confidentiality and integrity of this external system?

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

Answer: A

NEW QUESTION 682
- (Exam Topic 14)
What is the FIRST step required in establishing a records retention program?

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

Answer: D

NEW QUESTION 687
- (Exam Topic 14)
If virus infection is suspected, which of the following is the FIRST step for the user to take?

A. Unplug the computer from the network.
B. Save the opened files and shutdown the computer.
C. Report the incident to service desk.
D. Update the antivirus to the latest version.

Answer: C

NEW QUESTION 692
- (Exam Topic 14)
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

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

Answer: C

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

NEW QUESTION 694
- (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 696
- (Exam Topic 14)
Which of the following security testing strategies is BEST suited for companies with low to moderate security maturity?

A. Load Testing
B. White-box testing
C. Black -box testing
D. Performance testing

Answer: B

NEW QUESTION 697
- (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 701
- (Exam Topic 14)
In fault-tolerant systems, what do rollback capabilities permit?

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

Answer: A

NEW QUESTION 704
- (Exam Topic 14)
Which of the following is the MOST important reason for timely installation of software patches?

A. Attackers may be conducting network analysis.
B. Patches ere only available for a specific time.
C. Attackers reverse engineer the exploit from the patch.
D. Patches may not be compatible with proprietary software

Answer: C

NEW QUESTION 705
- (Exam Topic 14)
An organization implements a Remote Access Server (RAS). Once users correct to the server, digital certificates are used to authenticate their identity. What type of Extensible Authentication Protocol (EAP) would the organization use dring this authentication?

A. Transport layer security (TLS)
B. Message Digest 5 (MD5)
C. Lightweight Extensible Authentication Protocol (EAP)
D. Subscriber Identity Module (SIM)

Answer: A

NEW QUESTION 706
- (Exam Topic 14)
Which of the following is the BEST identity-as-a-service (IDaaS) solution for validating users?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAM.)
C. Single Sign-on (SSO)
D. Open Authentication (OAuth)

Answer: A

NEW QUESTION 711
- (Exam Topic 14)
Which of the following is MOST critical in a contract in a contract for data disposal on a hard drive with a third party?

A. Authorized destruction times
B. Allowed unallocated disk space
C. Amount of overwrites required
D. Frequency of recovered media

Answer: C

NEW QUESTION 713
- (Exam Topic 14)
What is the BEST way to correlate large volumes of disparate data sources in a Security Operations Center (SOC) environment?

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

Answer: B

NEW QUESTION 718

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

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

Answer: C

NEW QUESTION 723
- (Exam Topic 14)
Assume that a computer was powered off when an information security professional arrived at a crime scene. Which of the following actions should be performed after the crime scene is isolated?

A. Turn the computer on and collect volatile data.
B. Turn the computer on and collect network information.
C. Leave the computer off and prepare the computer for transportation to the laboratory
D. Remove the hard drive, prepare it for transportation, and leave the hardware ta the scene.

Answer: C

NEW QUESTION 724
- (Exam Topic 14)
Digital certificates used transport Layer security (TLS) support which of the following?

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

Answer: A

NEW QUESTION 729
- (Exam Topic 14)
Which of the following threats exists with an implementation of digital signatures?

A. Spoofing
B. Substitution
C. Content tampering
D. Eavesdropping

Answer: A

NEW QUESTION 731
- (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 733
- (Exam Topic 14)
Additional padding may be added to the Encapsulating security protocol (ESP) trailer to provide which of the following?

A. Data origin authentication
B. Partial traffic flow confidentiality
C. protection ao>ainst replay attack
D. Access control

Answer: C

NEW QUESTION 734
- (Exam Topic 14)
An analysis finds unusual activity coming from a computer that was thrown away several months prior, which of the following steps ensure the proper removal of the system?

A. Deactivation
B. Decommission
C. Deploy
D. Procure

Answer: B

NEW QUESTION 736
- (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 740
- (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 743
- (Exam Topic 14)
Which of the following media is least problematic with data remanence?

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

Answer: C

NEW QUESTION 748
- (Exam Topic 14)
What is the best way for mutual authentication of devices belonging to the same organization?

A. Token
B. Certificates
C. User ID and passwords
D. Biometric

Answer: A

Explanation:
Reference: https://books.google.com.pk/books?id=bb0re6h8JPAC&pg=PA637&lpg=PA637&dq=CISSP+for+mutual+auth

NEW QUESTION 749
- (Exam Topic 14)
Which of the following initiates the system recovery phase of a disaster recovery plan?

A. Evacuating the disaster site
B. Assessing the extent of damage following the disaster
C. Issuing a formal disaster declaration
D. Activating the organization's hot site

Answer: C

NEW QUESTION 750
- (Exam Topic 14)
An organization is required to comply with the Payment Card Industry Data Security Standard (PCI-DSS), what is the MOST effective approach to safeguard digital and paper media that contains cardholder data?

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

Answer: C

NEW QUESTION 751
- (Exam Topic 14)
During a recent assessment an organization has discovered that the wireless signal can be detected outside the campus area. What logical control should be implemented in order to BFST protect One confidentiality of information traveling One wireless transmission media?

A. Configure a firewall to logically separate the data at the boundary.
B. Configure the Access Points (AP) to use Wi-Fi Protected Access 2 (WPA2) encryption.
C. Disable the Service Set Identifier (SSID) broadcast on the Access Points (AP).
D. Perform regular technical assessments on the Wireless Local Area Network (WLAN).

Answer: B

NEW QUESTION 753
- (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 755
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

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

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