ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 15)
What is the FIRST step when developing an Information Security Continuous Monitoring (ISCM) program?

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

Answer: D

NEW QUESTION 3
- (Exam Topic 15)
Which of the following is an important requirement when designing a secure remote access system?

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

Answer: C

NEW QUESTION 4
- (Exam Topic 15)
In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

A. Organizational Security Policy
B. Security Target (ST)
C. Protection Profile (PP)
D. Target of Evaluation (TOE)

Answer: C

NEW QUESTION 5
- (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 6
- (Exam Topic 15)
Which of the following virtual network configuration options is BEST to protect virtual machines (VM)?

A. Traffic filtering
B. Data encryption
C. Data segmentation
D. Traffic throttling

Answer: D

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

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

Answer: A

NEW QUESTION 8
- (Exam Topic 15)
What is a use for mandatory access control (MAC)?

A. Allows for labeling of sensitive user accounts for access control
B. Allows for mandatory user identity and passwords based on sensitivity
C. Allows for mandatory system administrator access control over objects
D. Allows for object security based on sensitivity represented by a label

Answer: D

NEW QUESTION 9
- (Exam Topic 15)
he security organization is loading for a solution that could help them determine with a strong level of confident that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 15)
Which of the following 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 10
- (Exam Topic 15)
Which of the following routing protocols is used to exchange route information between public autonomous systems?

A. OSPF
B. BGP
C. EIGRP
D. RIP

Answer: B

NEW QUESTION 14
- (Exam Topic 15)
A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the
BEST design approach to securing this environment?

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

Answer: B

NEW QUESTION 18
- (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 20
- (Exam Topic 15)
Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

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

Answer: A

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

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

Answer: D

NEW QUESTION 26
- (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 31
- (Exam Topic 15)
A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

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

Answer: C

NEW QUESTION 34
- (Exam Topic 15)
Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-system gracefully handle invalid input?

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

Answer: B

NEW QUESTION 39
- (Exam Topic 15)
To minimize the vulnerabilities of a web-based application, which of the following FIRST actions will lock down the system and minimize the risk of an attack?

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

Answer: D

NEW QUESTION 40
- (Exam Topic 15)
An organization wants to define its physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

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

Answer: A

NEW QUESTION 43
- (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 46
- (Exam Topic 15)
Which of the following is the strongest physical access control?

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

Answer: D

NEW QUESTION 47
- (Exam Topic 15)
What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

A. ICS often do not have availability requirements.
B. ICS are often isolated and difficult to access.
C. ICS often run on UNIX operating systems.
D. ICS are often sensitive to unexpected traffic.

Answer: B

NEW QUESTION 49
- (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 50
- (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 55
- (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 56
- (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 59
- (Exam Topic 15)
What is the P R IM A R Y reason criminal law is difficult to enforce when dealing with cyber-crime?

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

Answer: D

NEW QUESTION 63
- (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 68
- (Exam Topic 15)
Which of the following is the MOST effective method of detecting vulnerabilities in web-based applications early in the secure Software Development Life Cycle (SDLC)?

A. Web application vulnerability scanning
B. Application fuzzing
C. Code review
D. Penetration testing

Answer: C

NEW QUESTION 73
- (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 74
- (Exam Topic 15)
The Rivest-Shamir-Adleman (RSA) algorithm is BEST suited for which of the following operations?

A. Bulk data encryption and decryption
B. One-way secure hashing for user and message authentication
C. Secure key exchange for symmetric cryptography
D. Creating digital checksums for message integrity

Answer: C

NEW QUESTION 76
- (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 79
- (Exam Topic 15)
Which of the following uses the destination IP address to forward packets?

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

Answer: C

NEW QUESTION 81
- (Exam Topic 15)
A software developer installs a game on their organization-provided smartphone. Upon installing the game, the software developer is prompted to allow the game access to call logs, Short Message Service (SMS) messaging, and Global Positioning System (GPS) location data. What has the game MOST likely introduced to the smartphone?

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

Answer: B

NEW QUESTION 83
- (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 88
- (Exam Topic 15)
What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

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

Answer: A

NEW QUESTION 92
- (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 94
- (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 99

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

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

Answer: B

NEW QUESTION 104
- (Exam Topic 15)
What method could be used to prevent passive attacks against secure voice communications between an organization and its vendor?

A. Encryption in transit
B. Configure a virtual private network (VPN)
C. Configure a dedicated connection
D. Encryption at rest

Answer: A

NEW QUESTION 106
- (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 108
- (Exam Topic 15)
Which element of software supply chain management has the GREATEST security risk to organizations?

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

Answer: B

NEW QUESTION 112
- (Exam Topic 15)
Who should formulate conclusions from a particular digital fore Ball, Submit a Toper Of Tags, and the results?

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

Answer: B

NEW QUESTION 117
- (Exam Topic 15)
Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

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

Answer: C

NEW QUESTION 121
- (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 125
- (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 126
- (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 130
- (Exam Topic 15)
The disaster recovery (DR) process should always include

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

Answer: A

NEW QUESTION 132
- (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 134
- (Exam Topic 15)
Which of the following phases in the software acquisition process does developing evaluation criteria take place?

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

Answer: D

NEW QUESTION 135
- (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 138
- (Exam Topic 15)
When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

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

Answer: B

NEW QUESTION 140
- (Exam Topic 15)
What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

A. Configuration management (CM)
B. Information Rights Management (IRM)
C. Policy creation
D. Data classification

Answer: D

NEW QUESTION 142
- (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 146
- (Exam Topic 15)
Which of the following is the MOST common cause of system or security failures?

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

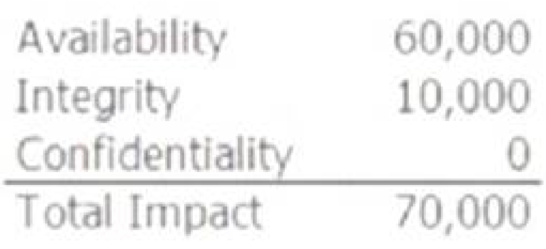
Answer: D

NEW QUESTION 151
- (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 152
- (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 153
- (Exam Topic 15)
A client server infrastructure that provides user-to-server authentication describes which one of the following?

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

Answer: B

NEW QUESTION 156
- (Exam Topic 15)
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 159
- (Exam Topic 15)
What is the BEST way to restrict access to a file system on computing systems?

A. Allow a user group to restrict access.
B. Use a third-party tool to restrict access.
C. Use least privilege at each level to restrict access.
D. Restrict access to all users.

Answer: C

NEW QUESTION 161
- (Exam Topic 15)
Which of the following determines how traffic should flow based on the status of the infrastructure layer?

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

Answer: A

NEW QUESTION 162
- (Exam Topic 15)
Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management
decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

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

Answer: A

NEW QUESTION 165
- (Exam Topic 15)
Which of the following BEST represents a defense in depth concept?

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

Answer: C

NEW QUESTION 166
- (Exam Topic 15)
Which of the following are the B EST characteristics of security metrics?

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

Answer: D

NEW QUESTION 170
- (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 173
- (Exam Topic 15)
Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

A. Transport Layer
B. Data Link and Physical Layers
C. Application, Presentation, and Session Layers
D. Session and Network Layers

Answer: B

NEW QUESTION 176
- (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 181
- (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 184
- (Exam Topic 15)
The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

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

Answer: B

NEW QUESTION 185
- (Exam Topic 15)
An information technology (IT) employee who travels frequently to various ies remotely to an organization' the following solutions BEST serves as a secure control mechanism to meet the organization's requirements? to troubleshoot p Which of the following solutions BEST serves as a secure control mechanisn to meet the organization's requirements?

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

Answer: D

NEW QUESTION 186
- (Exam Topic 15)
Which one of the following BEST protects vendor accounts that are used for emergency maintenance?

A. Encryption of routing tables

B. Vendor access should be disabled until needed
C. Role-based access control (RBAC)
D. Frequent monitoring of vendor access

Answer: B

NEW QUESTION 187
- (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 192
- (Exam Topic 15)
Which of the following is the BEST way to determine the success of a patch management process?

A. Analysis and impact assessment
B. Auditing and assessment
C. Configuration management (CM)
D. Change management

Answer: A

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

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

Answer: B

NEW QUESTION 194
- (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 199
- (Exam Topic 15)
If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), which of the following becomes even MORE essential to the assurance of network?

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

Answer: C

NEW QUESTION 201
- (Exam Topic 15)
A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

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

Answer: B

NEW QUESTION 204

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

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

Answer: B

NEW QUESTION 209
- (Exam Topic 15)
Which of the following terms BEST describes a system which allows a user to log in and access multiple related servers and applications?

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

Answer: B

NEW QUESTION 211
- (Exam Topic 15)
Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

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

Answer: C

NEW QUESTION 215
- (Exam Topic 15)
Which of the following poses the GREATEST privacy risk to personally identifiable information (PII) when disposing of an office printer or copier?

A. The device could contain a document with PII on the platen glass
B. Organizational network configuration information could still be present within the device
C. A hard disk drive (HDD) in the device could contain PII
D. The device transfer roller could contain imprints of PII

Answer: B

NEW QUESTION 216
- (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 218
- (Exam Topic 15)
Dumpster diving is a technique used in which stage of penetration testing methodology?

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

Answer: B

NEW QUESTION 223
- (Exam Topic 15)
When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network. Which of the following will BEST help secure the VoIP network?

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

Answer: A

NEW QUESTION 227
- (Exam Topic 15)
In a multi-tenant cloud environment, what approach will secure logical access to assets?

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

Answer: D

NEW QUESTION 231
- (Exam Topic 15)
After the INITIAL input o f a user identification (ID) and password, what is an authentication system that prompts the user for a different response each time the user logs on?

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

Answer: C

NEW QUESTION 233
- (Exam Topic 15)
An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

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

Answer: B

NEW QUESTION 234
- (Exam Topic 15)
An organization has discovered that organizational data is posted by employees to data storage accessible to the general public. What is the PRIMARY step an organization must take
to ensure data is properly protected from public release?

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

Answer: C

NEW QUESTION 238
- (Exam Topic 15)
An information security administrator wishes to block peer-to-peer (P2P) traffic over Hypertext Transfer Protocol (HTTP) tunnels. Which of the following layers of the Open Systems Interconnection (OSI) model requires inspection?

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

Answer: A

NEW QUESTION 242
- (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 243
- (Exam Topic 15)
An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

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

Answer: D

NEW QUESTION 246
- (Exam Topic 15)
What BEST describes the confidentiality, integrity, availability triad?

A. A tool used to assist in understanding how to protect the organization's data
B. The three-step approach to determine the risk level of an organization
C. The implementation of security systems to protect the organization's data
D. A vulnerability assessment to see how well the organization's data is protected

Answer: C

NEW QUESTION 248
- (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 252
- (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 256
- (Exam Topic 15)
Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management’s directive?

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

Answer: B

NEW QUESTION 259
- (Exam Topic 15)
Commercial off-the-shelf (COTS) software presents which of the following additional security concerns?

A. Vendors take on the liability for COTS software vulnerabilities.
B. In-house developed software is inherently less secure.
C. Exploits for COTS software are well documented and publicly available.
D. COTS software is inherently less secure.

Answer: C

NEW QUESTION 263
- (Exam Topic 15)
In setting expectations when reviewing the results of a security test, which of the following statements is MOST important to convey to reviewers?

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

Answer: C

NEW QUESTION 264

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

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

Answer: C

NEW QUESTION 268
- (Exam Topic 15)
A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks, What is the MOST efficient option used to prevent buffer overflow attacks?

A. Process isolation
B. Address Space Layout Randomization (ASLR)
C. Processor states
D. Access control mechanisms

Answer: B

NEW QUESTION 272
- (Exam Topic 15)
Which of the following is MOST appropriate to collect evidence of a zero-day attack?

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

Answer: A

NEW QUESTION 277
- (Exam Topic 15)
A hospital has allowed virtual private networking (VPN) access to remote database developers. Upon auditing the internal firewall configuration, the network administrator discovered that split-tunneling was enabled. What is the concern with this configuration?

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

Answer: C

NEW QUESTION 280
- (Exam Topic 15)
Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

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

Answer: C

NEW QUESTION 284
- (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 285
- (Exam Topic 15)
A Chief Information Security Officer (CISO) of a firm which decided to migrate to cloud has been tasked with ensuring an optimal level of security. Which of the following would be the FIRST consideration?

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

Answer: A

NEW QUESTION 289
- (Exam Topic 15)
Which of the following is the PRIMARY purpose of due diligence when an organization embarks on a merger or acquisition?

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

Answer: A

NEW QUESTION 294
- (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 297
- (Exam Topic 15)
Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this TAM action?

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

Answer: A

NEW QUESTION 302
- (Exam Topic 15)
The acquisition of personal data being obtained by a lawful and fair means is an example of what principle?

A. Data Quality Principle
B. Openness Principle
C. Purpose Specification Principle
D. Collection Limitation Principle

Answer: D

NEW QUESTION 307
- (Exam Topic 15)
An organization is planning to have an it audit of its as a Service (SaaS) application to demonstrate to external parties that the security controls around availability are designed. The audit report must also cover a certain period of time to show the operational effectiveness of the controls. Which Service Organization Control (SOC) report would BEST fit their needs?

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

Answer: D

NEW QUESTION 310
- (Exam Topic 15)
An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

A. Health Insurance Portability and Accountability Act (HIPAA)
B. Service Organization Control (SOC) 2
C. Payment Card Industry (PCI)
D. Information Assurance Technical Framework (IATF)

Answer: B

NEW QUESTION 312
- (Exam Topic 15)
A network security engineer needs to ensure that a security solution analyzes traffic for protocol manipulation and various sorts of common attacks. In addition, all Uniform Resource Locator (URL) traffic must be inspected and users prevented from browsing inappropriate websites. Which of the following solutions should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis?

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

Answer: B

NEW QUESTION 313
- (Exam Topic 15)
A company hired an external vendor to perform a penetration test ofa new payroll system. The company’s internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

A. Failure to perform interface testing
B. Failure to perform negative testing
C. Inadequate performance testing
D. Inadequate application level testing

Answer: A

NEW QUESTION 317
- (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 318
- (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 321
- (Exam Topic 15)
Which of the following is considered the FIRST step when designing an internal security control assessment?

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

Answer: D

NEW QUESTION 324
- (Exam Topic 15)
Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

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

Answer: D

NEW QUESTION 326
- (Exam Topic 15)
The Chief Information Security Officer (CISO) is concerned about business application availability. The organization was recently subject to a ransomware attack that resulted in the unavailability of applications and services for 10 working days that required paper-based running of all main business processes. There are now aggressive plans to enhance the Recovery Time Objective (RTO) and cater for more frequent data captures. Which of the following solutions should be implemented to fully comply to the new business requirements?

A. Virtualization
B. Antivirus
C. Process isolation
D. Host-based intrusion prevention system (HIPS)

Answer: A

NEW QUESTION 331
- (Exam Topic 15)
Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

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

Answer: B

NEW QUESTION 335
- (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 339
- (Exam Topic 15)
An organization recently suffered from a web-application attack that resulted in stolen user session cookie information. The attacker was able to obtain the information when a user's browser executed a script upon visiting a compromised website. What type of attack MOST likely occurred?

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

Answer: A

NEW QUESTION 342
- (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 346
- (Exam Topic 15)
Which of the following types of datacenter architectures will MOST likely be used in a large SDN and can be extended beyond the datacenter?

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

Answer: B

NEW QUESTION 348
- (Exam Topic 15)
If an employee transfers from one role to another, which of the following actions should this trigger within the identity and access management (IAM) lifecycle?

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

Answer: B

NEW QUESTION 350

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

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

Answer: D

NEW QUESTION 353
- (Exam Topic 15)
What is the MOST significant benefit of role-based access control (RBAC)?

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

Answer: A

NEW QUESTION 356
- (Exam Topic 15)
When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

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

Answer: C

NEW QUESTION 357
- (Exam Topic 15)
In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

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

Answer: D

NEW QUESTION 360
- (Exam Topic 15)
Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

A. Change driver
B. Change implementer
C. Program sponsor
D. Project manager

Answer: D

NEW QUESTION 361
- (Exam Topic 15)
What is the FIRST step in risk management?

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

Answer: C

NEW QUESTION 364
- (Exam Topic 15)
A subscription service which provides power, climate control, raised flooring, and telephone wiring but NOT the computer and peripheral equipment is BEST described as a:

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

Answer: C

NEW QUESTION 365
- (Exam Topic 15)
Which of the following is a correct feature of a virtual local area network (VLAN)?

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

Answer: A

NEW QUESTION 367
- (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 368
- (Exam Topic 15)
Which of the following is the MOST appropriate technique for destroying magnetic platter style hard disk drives (HDD) containing data with a "HIGH" security categorization?

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

Answer: D

NEW QUESTION 369
- (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 374
- (Exam Topic 15)
Which of the following are the three MAIN categories of security controls?

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

Answer: A

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

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

Answer: C

NEW QUESTION 384
- (Exam Topic 15)
What action should be taken by a business line that is unwilling to accept the residual risk in a system after implementing compensating controls?

A. Notify the audit committee of the situation.
B. Purchase insurance to cover the residual risk.
C. Implement operational safeguards.

D. Find another business line willing to accept the residual risk.

Answer: B

NEW QUESTION 389
- (Exam Topic 15)
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

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

Answer: C

NEW QUESTION 390
- (Exam Topic 15)
When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

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

Answer: B

NEW QUESTION 395
- (Exam Topic 15)
The quality assurance (QA) department is short-staffed and is unable to test all modules before the anticipated release date of an application. What security control is MOST likely to be violated?

A. Separation of environments
B. Program management
C. Mobile code controls
D. Change management

Answer: D

NEW QUESTION 400
- (Exam Topic 15)
Which of the following statements BEST describes least privilege principle in a cloud environment?

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

Answer: B

NEW QUESTION 404
- (Exam Topic 15)
A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS).
Which of the following factors leads the company to choose an IDaaS as their solution?

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

Answer: B

NEW QUESTION 405
- (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 406

- (Exam Topic 15)
Which technique helps system designers consider potential security concerns of their systems and applications?

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

Answer: B

NEW QUESTION 408
- (Exam Topic 15)
The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

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

Answer: D

NEW QUESTION 411
- (Exam Topic 15)
Which of the following BEST describes the purpose of Border Gateway Protocol (BGP)?

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

Answer: B

NEW QUESTION 412
- (Exam Topic 15)
A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

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

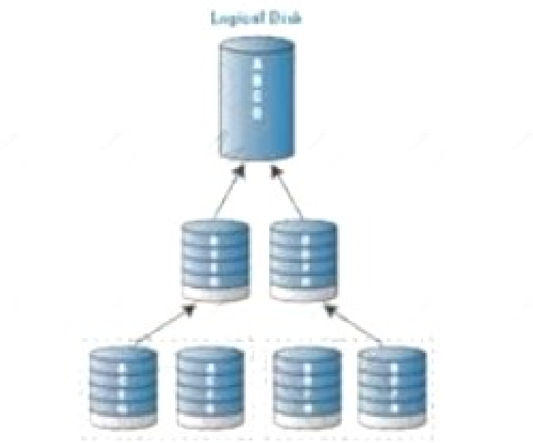
Answer: B

NEW QUESTION 413
- (Exam Topic 15)
What are the first two components of logical access control?

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

Answer: B

NEW QUESTION 417
- (Exam Topic 15)
Which Redundant Array c/ Independent Disks (RAID) Level does the following diagram represent?



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

Answer: D

NEW QUESTION 419
- (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 420
- (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 424
- (Exam Topic 15)
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

A. nslookup
B. show config
C. netstat
D. show interface
E. show counters

Answer: D

NEW QUESTION 426
- (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 429
- (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 433
- (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 437
- (Exam Topic 15)
When telephones in a city are connected by a single exchange, the caller can only connect with the switchboard operator. The operator then manually connects the call.
This is an example of which type of network topology?

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

Answer: A

NEW QUESTION 439
- (Exam Topic 15)
The MAIN purpose of placing a tamper seal on a computer system's case is to:

A. raise security awareness.
B. detect efforts to open the case.
C. expedite physical auditing.
D. make it difficult to steal internal components.

Answer: A

NEW QUESTION 443
- (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 444
- (Exam Topic 15)
Which of the following has the responsibility of information technology (IT) governance?

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

Answer: A

NEW QUESTION 446
- (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 448
- (Exam Topic 15)
An employee's home address should be categorized according to which of the following references?

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

Answer: B

NEW QUESTION 449
- (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 450

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

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

Answer: C

NEW QUESTION 451
- (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 456
- (Exam Topic 15)
In software development, developers should use which type of queries to prevent a Structured Query Language (SQL) injection?

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

Answer: A

NEW QUESTION 458
- (Exam Topic 15)
An organization wants a service provider to authenticate users via the users' organization domain credentials. Which markup language should the organization's security personnel use to support the integration?

A. Security Assertion Markup Language (SAML)
B. YAML Ain't Markup Language (YAML)
C. Hypertext Markup Language (HTML)
D. Extensible Markup Language (XML)

Answer: A

NEW QUESTION 459
- (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 464
- (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 465
- (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 468
- (Exam Topic 15)
Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

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

Answer: A

NEW QUESTION 471
- (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 475
- (Exam Topic 15)
The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

A. Data loss protection (DLP)
B. Intrusion detection
C. Vulnerability scanner
D. Information Technology Asset Management (ITAM)

Answer: D

NEW QUESTION 479
- (Exam Topic 15)
To monitor the security of buried data lines inside the perimeter of a facility, which of the following is the MOST effective control?

A. Fencing around the facility with closed-circuit television (CCTV) cameras at all entry points
B. Ground sensors installed and reporting to a security event management (SEM) system
C. Steel casing around the facility ingress points
D. regular sweeps of the perimeter, including manual inspection of the cable ingress points

Answer: D

NEW QUESTION 480
- (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 482
- (Exam Topic 15)
Which of the following is the name of an individual or group that is impacted by a change?

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

Answer: B

NEW QUESTION 485
- (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 490
- (Exam Topic 15)
Which of the following is a security weakness in the evaluation of common criteria (CC) products?

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

Answer: A

NEW QUESTION 493
- (Exam Topic 15)
What is the MAIN purpose of a security assessment plan?

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

Answer: B

NEW QUESTION 497
- (Exam Topic 15)
Which of the following protects personally identifiable information (PII) used by financial services organizations?

A. National Institute of Standards and Technology (NIST) SP 800-53
B. Gramm-Leach-Bliley Act (GLBA)
C. Payment Card Industry Data Security Standard (PCI-DSS)
D. Health Insurance Portability and Accountability Act (HIPAA)

Answer: B

NEW QUESTION 502
- (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 507
- (Exam Topic 15)
What is the overall goal of software security testing?

A. Identifying the key security features of the software
B. Ensuring all software functions perform as specified
C. Reducing vulnerabilities within a software system
D. Making software development more agile

Answer: B

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

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

Answer: A

NEW QUESTION 512
- (Exam Topic 15)
What is the PRIMARY reason that a bit-level copy is more desirable than a file-level copy when replicating a hard drive's contents for an e-discovery investigation?

A. Files that have been deleted will be transferred.

B. The file and directory structure is retained.
C. File-level security settings will be preserved.
D. The corruption of files is less likely.

Answer: A

NEW QUESTION 514
- (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 516
- (Exam Topic 15)
Which of the following BEST describes when an organization should conduct a black box security audit on a new software product?

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

Answer: B

NEW QUESTION 518
- (Exam Topic 15)
Which of the following techniques evaluates the secure Bet principles of network or software architectures?

A. Threat modeling
B. Risk modeling
C. Waterfall method
D. Fuzzing

Answer: A

NEW QUESTION 520
- (Exam Topic 15)
Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

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

Answer: C

NEW QUESTION 522
- (Exam Topic 15)
An organization outgrew its internal data center and is evaluating third-party hosting facilities. In this evaluation, which of the following is a PRIMARY factor for selection?

A. Facility provides an acceptable level of risk
B. Facility provides disaster recovery (DR) services
C. Facility provides the most cost-effective solution
D. Facility has physical access protection measures

Answer: C

NEW QUESTION 527
- (Exam Topic 15)
A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to on and security However, an attacker was able to spoof a registered account on the network and query the SAML provider.
What is the MOST common attack leverage against this flaw?

A. Attacker forges requests to authenticate as a different user.
B. Attacker leverages SAML assertion to register an account on the security domain.
C. Attacker conducts denial-of-service (DoS) against the security domain by authenticating as the same user repeatedly.
D. Attacker exchanges authentication and authorization data between security domains.

Answer: A

NEW QUESTION 531

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

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

Answer: D

NEW QUESTION 536
- (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 538
- (Exam Topic 15)
Which of the following BEST describes centralized identity management?

A. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
B. Service providers agree to integrate identity system recognition across organizational boundaries.
C. Service providers identify an entity by behavior analysis versus an identification factor.
D. Service providers perform as both the credential and identity provider (IdP).

Answer: B

NEW QUESTION 540
- (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 542
- (Exam Topic 15)
Which of the following contributes MOST to the effectiveness of a security officer?

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

Answer: A

NEW QUESTION 544
- (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 547
- (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 549
- (Exam Topic 15)
Which of the following is a standard Access Control List (ACL) element that enables a router to filter Internet traffic?

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

Answer: B

NEW QUESTION 551
- (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 555
- (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 556
- (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 559
- (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 564
- (Exam Topic 15)
Which is MOST important when negotiating an Internet service provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over Internet Protocol (VoIP) services?

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

Answer: B

NEW QUESTION 569
- (Exam Topic 15)
What part of an organization’s strategic risk assessment MOST likely includes information on items affecting the success of the organization?

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

Answer: A

NEW QUESTION 571
- (Exam Topic 15)
A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

A. Network is flooded with communication traffic by the attacker.
B. Organization loses control of their network devices.
C. Network management communications is disrupted.
D. Attacker accesses sensitive information regarding the network topology.

Answer: B

NEW QUESTION 574
- (Exam Topic 15)
Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

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

Answer: C

NEW QUESTION 578
- (Exam Topic 15)
An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a
per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

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

Answer: A

NEW QUESTION 579
- (Exam Topic 15)
An organization contracts with a consultant to perform a System Organization Control (SOC) 2 audit on their internal security controls. An auditor documents a finding related to an Application Programming Interface (API) performing an action that is not aligned with the scope or objective of the system. Which trust service principle would be MOST applicable in this situation?

A. Processing Integrity
B. Availability
C. Confidentiality
D. Security

Answer: B

NEW QUESTION 582
- (Exam Topic 15)
Which of the following should exist in order to perform a security audit?

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

Answer: D

NEW QUESTION 583
- (Exam Topic 15)
While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team?

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

Answer: C

NEW QUESTION 588
- (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 590
- (Exam Topic 15)
When recovering from an outage, what is the Recovery Point Objective (RPO), in terms of data recovery?

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

Answer: B

NEW QUESTION 591
- (Exam Topic 15)
What should be used to determine the risks associated with using Software as a Service (SaaS) for collaboration and email?

A. Cloud access security broker (CASB)
B. Open Web Application Security Project (OWASP)
C. Process for Attack Simulation and Threat Analysis (PASTA)
D. Common Security Framework (CSF)

Answer: A

NEW QUESTION 592
- (Exam Topic 15)
Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

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

Answer: D

NEW QUESTION 596
- (Exam Topic 15)
The initial security categorization should be done early in the system life cycle and should be reviewed periodically. Why is it important for this to be done correctly?

A. It determines the security requirements.
B. It affects other steps in the certification and accreditation process.
C. It determines the functional and operational requirements.
D. The system engineering process works with selected security controls.

Answer: B

NEW QUESTION 598
- (Exam Topic 15)
A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

A. Update the service level agreement (SLA) to provide the organization the right to audit the vendor.
B. Update the service level agreement (SLA) to require the vendor to provide security capabilities.
C. Update the contract so that the vendor is obligated to provide security capabilities.
D. Update the contract to require the vendor to perform security code reviews.

Answer: C

NEW QUESTION 601
- (Exam Topic 15)
A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

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

Answer: D

NEW QUESTION 606
- (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 608
- (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 612
- (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 614
- (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 619
- (Exam Topic 15)
Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

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

Answer: B

NEW QUESTION 623
- (Exam Topic 14)
Which of the following is the BEST technique to facilitate secure software development?

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

Answer: A

NEW QUESTION 625
- (Exam Topic 15)
A security professional has been requested by the Board of Directors and Chief Information Security Officer (CISO) to perform an internal and external penetration

test. What is the BEST course of action?

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

Answer: D

NEW QUESTION 630
- (Exam Topic 14)
Which of the following media is LEAST problematic with data remanence?

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

Answer: A

NEW QUESTION 635
- (Exam Topic 14)
What should an auditor do when conducting a periodic audit on media retention?

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

Answer: A

NEW QUESTION 636
- (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 640
- (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 643
- (Exam Topic 14)
An organization is considering outsourcing applications and data to a Cloud Service Provider (CSP). Which of the following is the MOST important concern regarding privacy?

A. The CSP determines data criticality.
B. The CSP provides end-to-end encryption services.
C. The CSP’s privacy policy may be developer by the organization.
D. The CSP may not be subject to the organization’s country legation.

Answer: D

NEW QUESTION 645
- (Exam Topic 14)
An organization has implemented a new backup process which protects confidential data by encrypting the information stored on backup tapes. Which of the following is a MAJOR data confidentiality concern after the implementation of this new backup process?

A. Tape backup rotation
B. Pre-existing backup tapes
C. Tape backup compression
D. Backup tape storage location

Answer: D

NEW QUESTION 648
- (Exam Topic 14)
Why should Open Web Application Security Project (OWASP) Application Security Verification standards (ASVS) Level 1 be considered a MINIMUM level of protection for any web application?

A. ASVS Level 1 ensures that applications are invulnerable to OWASP top 10 threats.
B. Opportunistic attackers will look for any easily exploitable vulnerable applications.
C. Most regulatory bodies consider ASVS Level 1 as a baseline set of controls for applications.
D. Securing applications at ASVS Level 1 provides adequate protection for sensitive data.

Answer: B

NEW QUESTION 651
- (Exam Topic 14)
Internet protocol security (IPSec), point-to-point tunneling protocol (PPTP), and secure sockets Layer (SSL) all use Which of the following to prevent replay attacks?

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

Answer: C

NEW QUESTION 652
- (Exam Topic 14)
Which of the following techniques is effective to detect taps in fiber optic cables?

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

Answer: B

NEW QUESTION 657
- (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 662
- (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 666
- (Exam Topic 14)
A corporate security policy specifies that all devices on the network must have updated operating system patches and anti-malware software. Which technology should be used to enforce this policy?

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

Answer: D

NEW QUESTION 668
- (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 670
- (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 673
- (Exam Topic 14)
How can an attacker exploit overflow to execute arbitrary code?

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

Answer: A

NEW QUESTION 677
- (Exam Topic 14)
Which of the following types of data would be MOST difficult to detect by a forensic examiner?

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

Answer: C

NEW QUESTION 681
- (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 686
- (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 689
- (Exam Topic 14)
An organization has a short-term agreement with a public Cloud Service Provider (CSP). Which of the following BEST protects sensitive data once the agreement expires and the assets are reused?

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

Answer: C

NEW QUESTION 692
- (Exam Topic 14)
What is the MOST common component of a vulnerability management framework?

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

Answer: B

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

NEW QUESTION 693
- (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 694
- (Exam Topic 14)
Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

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

Answer: A

NEW QUESTION 699
- (Exam Topic 14)
Which of the following practices provides the development team with a definition of security and identification of threats in designing software?

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

Answer: C

NEW QUESTION 701
- (Exam Topic 14)
What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

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

Answer: C

NEW QUESTION 706
- (Exam Topic 14)
Which of the following authorization standards is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM)?

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

Answer: B

NEW QUESTION 708
- (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 710
- (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 714
- (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 715
- (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 716
- (Exam Topic 14)
What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

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

Answer: B

NEW QUESTION 721
- (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 724
- (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 728
- (Exam Topic 14)
Which of the following is the BEST defense against password guessing?

A. Limit external connections to the network.
B. Disable the account after a limited number of unsuccessful attempts.

C. Force the password to be changed after an invalid password has been entered.
D. Require a combination of letters, numbers, and special characters in the password.

Answer: D

NEW QUESTION 731
- (Exam Topic 14)
A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

A. No, because the encryption solution is internal to the cloud provider.
B. Yes, because the cloud provider meets all regulations requirements.
C. Yes, because the cloud provider is GDPR compliant.
D. No, because the cloud provider is not certified to host government data.

Answer: B

NEW QUESTION 735
- (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 737
- (Exam Topic 14)
When a flaw in Industrial control (ICS) software is discovered, what is the GREATEST impediment to deploying a patch?

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

Answer: D

NEW QUESTION 741
- (Exam Topic 14)
What is the PRIMARY benefit of analyzing the partition layout of a hard disk volume when performing forensic analysis?

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

Answer: A

NEW QUESTION 742
- (Exam Topic 14)
How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

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

Answer: A

NEW QUESTION 745
- (Exam Topic 14)
Which type of fire alarm system sensor is intended to detect fire at its earliest stage?

A. Ionization
B. Infrared
C. Thermal
D. Photoelectric

Answer: A

NEW QUESTION 749

- (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 752
- (Exam Topic 14)
A vehicle of a private courier company that transports backup data for offsite storage was robbed while in transport backup data for offsite was robbed while in transit. The incident management team is now responsible to estimate the robbery, which of the following would help the incident management team to MOST effectively analyze the business impact of the robbery?

A. Log of backup administrative actions
B. Log of the transported media and its classification marking
C. Log of the transported media and Its detailed contents
D. Log of backed up data and their respective data custodians

Answer: B

NEW QUESTION 756
- (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 759
- (Exam Topic 14)
The MAIN task of promoting security for Personal Computers (PC) is

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

Answer: C

NEW QUESTION 762
- (Exam Topic 14)
Utilizing a public wireless Local Area network (WLAN) to connect to a private network should be done only
in which of the following situations?

A. Extensible Authentication Protocol (EAP) is utilized to authenticate the user.
B. The client machine has a personal firewall and utilizes a Virtual Private Network (VPN) to connect to the network.
C. The client machine has antivirus software and has been seamed to determine if unauthorized ports are open.
D. The wireless Access Point (AP) is placed in the internal private network.

Answer: A

NEW QUESTION 764
- (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 766
- (Exam Topic 14)
Which of the following can be used to calculate the loss event probability?

A. Total number of possible outcomes divided by frequency of outcomes
B. Number of outcomes divided by total number of possible outcomes
C. Number of outcomes multiplied by total number of possible outcomes
D. Total number of possible outcomes multiplied by frequency of outcomes

Answer: B

NEW QUESTION 771
- (Exam Topic 14)
Which of the following management processes allots ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

A. Compliance
B. Configuration
C. Identity
D. Patch

Answer: B

NEW QUESTION 773
- (Exam Topic 14)
Which of the following practices provides the development of security and identification of threats in designing software?

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

Answer: D

NEW QUESTION 776
- (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 779
- (Exam Topic 14)
When a system changes significantly, who is PRIMARILY responsible for assessing the security impact?

A. Chief Information Security Officer (CISO)
B. Information System Owner
C. Information System Security Officer (ISSO)
D. Authorizing Official

Answer: B

NEW QUESTION 780
- (Exam Topic 14)
A security engineer is designing a Customer Relationship Management (CRM) application for a third-party vendor. In which phase of the System Development Life Cycle (SDLC) will it be MOST beneficial to conduct a data sensitivity assessment?

A. Development / Acquisition
B. Initiation
C. Enumeration
D. Operation / Maintenance

Answer: B

NEW QUESTION 782
- (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 787
......

Relate Links

Contact us