ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

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

Answer: D

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

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

Answer: D

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

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

Answer: C

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

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

Answer: D

NEW QUESTION 6
- (Exam Topic 15)
Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless
Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

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

Answer: B

NEW QUESTION 7
- (Exam Topic 15)
A company is planning to implement a private cloud infrastructure. Which of the following recommendations will support the move to a cloud infrastructure?

A. Implement a virtual local area network (VLAN) for each department and create a separate subnet for each VLAN.
B. Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.

C. Implement a virtual local area network (VLAN) to logically separate the local area network (LAN) from the physical switches.
D. implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices and applications.

Answer: D

NEW QUESTION 8
- (Exam Topic 15)
Which of the following is fundamentally required to address potential security issues when initiating software development?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 15)
A large human resources organization wants to integrate their identity management with a trusted partner organization. The human resources organization wants to maintain the creation and management of the identities and may want to share with other partners in the future. Which of the following options BEST serves their needs?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 15)
Which of the following is a PRIMARY security weakness in the design of Domain Name System (DNS)?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 15)
A cybersecurity engineer has been tasked to research and implement an ultra-secure communications channel to protect the organization's most valuable intellectual property (IP). The primary directive in this initiative is to ensure there Is no possible way the communications can be intercepted without detection. Which of the following Is the only way to ensure this ‘outcome?

A. Diffie-Hellman key exchange
B. Symmetric key cryptography
C. [Public key infrastructure (PKI)
D. Quantum Key Distribution

Answer: C

NEW QUESTION 12
- (Exam Topic 15)
Which of the following is the FIRST step for defining Service Level Requirements (SLR)?

A. Creating a prototype to confirm or refine the customer requirements
B. Drafting requirements for the service level agreement (SLA)
C. Discussing technology and solution requirements with the customer
D. Capturing and documenting the requirements of the customer

Answer: D

NEW QUESTION 16
- (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 19
- (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 22
- (Exam Topic 15)
When reviewing the security logs, the password shown for an administrative login event was ' OR ' '1'='1' --. This is an example of which of the following kinds of attack?

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

Answer: B

NEW QUESTION 27
- (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 29
- (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 32
- (Exam Topic 15)
An organization needs a general purpose document to prove that its internal controls properly address security, availability, processing integrity, confidentiality or privacy risks. Which of the following reports is required?

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

Answer: C

NEW QUESTION 34
- (Exam Topic 15)
Which of the following is the MOST effective preventative method to identify security flaws in software?

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

Answer: B

NEW QUESTION 39
- (Exam Topic 15)
Which of the following is the BEST way to protect against Structured Query language (SQL) injection?

A. Enforce boundary checking.
B. Ratfrict um of SELECT command.

C. Restrict HyperText Markup Language (HTML) source code
D. Use stored procedures.

Answer: D

NEW QUESTION 42
- (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 44
- (Exam Topic 15)
Which of the following types of firewall only examines the “handshaking” between packets before forwarding traffic?

A. Proxy firewalls
B. Host-based firewalls
C. Circuit-level firewalls
D. Network Address Translation (NAT) firewalls

Answer: C

NEW QUESTION 46
- (Exam Topic 15)
A digitally-signed e-mail was delivered over a wireless network protected with Wired Equivalent Privacy (WEP) protocol. Which of the following principles is at risk?

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

Answer: B

NEW QUESTION 47
- (Exam Topic 15)
Which of the following regulations dictates how data breaches are handled?

A. Sarbanes-Oxley (SOX)
B. National Institute of Standards and Technology (NIST)
C. Payment Card Industry Data Security Standard (PCI-DSS)
D. General Data Protection Regulation (GDPR)

Answer: D

NEW QUESTION 51
- (Exam Topic 15)
A security practitioner needs to implementation solution to verify endpoint security protections and operating system (0S) versions. Which of the following is the BEST solution to implement?

A. An intrusion prevention system (IPS)
B. An intrusion prevention system (IPS)
C. Network Access Control (NAC)
D. A firewall

Answer: B

NEW QUESTION 54
- (Exam Topic 15)
Which of the following examples is BEST to minimize the attack surface for a customer's private information?

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

Answer: A

NEW QUESTION 59
- (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 64
- (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 69
- (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 74
- (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 76
- (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 80
- (Exam Topic 15)
Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

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

Answer: A

NEW QUESTION 83
- (Exam Topic 15)
A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

A. Hybrid frequency band, service set identifier (SSID), and interpolation
B. Performance, geographic location, and radio signal interference
C. Facility size, intermodulation, and direct satellite service
D. Existing client devices, manufacturer reputation, and electrical interference

Answer: D

NEW QUESTION 88
- (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 91
- (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 96
- (Exam Topic 15)
A software development company has a short timeline in which to deliver a software product. The software development team decides to use open-source software libraries to reduce the development time. What concept should software developers consider when using open-source software libraries?

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

Answer: A

NEW QUESTION 99
- (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 101
- (Exam Topic 15)
Which of the following is a Key Performance Indicator (KPI) for a security training and awareness program?

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

Answer: B

NEW QUESTION 103
- (Exam Topic 15)
Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

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

Answer: D

NEW QUESTION 107
- (Exam Topic 15)
Which of the following is the MOST appropriate control for asset data labeling procedures?

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

Answer: C

NEW QUESTION 108
- (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 111
- (Exam Topic 15)
Which of the following is the MOST secure password technique?

A. Passphrase
B. One-time password
C. Cognitive password
D. dphertext

Answer: A

NEW QUESTION 116
- (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 119
- (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 121
- (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 124
- (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 126
- (Exam Topic 15)
A security professional has been assigned to assess a web application. The assessment report recommends switching to Security Assertion Markup Language

(SAML). What is the PRIMARY security benefit in switching to SAML?

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

Answer: B

NEW QUESTION 129
- (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 132
- (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 134
- (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 135
- (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 139
- (Exam Topic 15)
Security Software Development Life Cycle (SDLC) expects application code to be written In a consistent manner to allow ease of auditing and which of the following?

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

Answer: A

NEW QUESTION 141
- (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 146
- (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 148
- (Exam Topic 15)
Which of the following is the PRIMARY issue when analyzing detailed log information?

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

Answer: D

NEW QUESTION 149
- (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 151
- (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 153
- (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 155
- (Exam Topic 15)
Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

A. File Integrity Checker
B. Security information and event management (SIEM) system
C. Audit Logs
D. Intrusion detection system (IDS)

Answer: A

NEW QUESTION 160
- (Exam Topic 15)
Data remanence is the biggest threat in which of the following scenarios?

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

Answer:

D

NEW QUESTION 162
- (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 164
- (Exam Topic 15)
What are the essential elements of a Risk Assessment Report (RAR)?

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

Answer: D

NEW QUESTION 169
- (Exam Topic 15)
An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

A. Default the user to not share any information.
B. Inform the user of the sharing feature changes after implemented.
C. Share only what the organization decides is best.
D. Stop sharing data with the other users.

Answer: D

NEW QUESTION 172
- (Exam Topic 15)
Which of the following is the BEST approach to implement multiple servers on a virtual system?

A. Implement multiple functions per virtual server and apply the same security configuration for each virtual server.
B. Implement one primary function per virtual server and apply high security configuration on the host operating system.
C. Implement one primary function per virtual server and apply individual security configuration for each virtual server.
D. Implement multiple functions within the same virtual server and apply individual security configurations to each function.

Answer: C

NEW QUESTION 177
- (Exam Topic 15)
Which of the following is required to verify the authenticity of a digitally signed document?

A. Digital hash of the signed document
B. Sender's private key
C. Recipient's public key
D. Agreed upon shared secret

Answer: A

NEW QUESTION 180
- (Exam Topic 15)
Which of the following is the PRIMARY goal of logical access controls?

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

Answer: C

NEW QUESTION 182
- (Exam Topic 15)
Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

A. Sniffing the traffic of a compromised host inside the network
B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network

C. A brute force password attack on the Secure Shell (SSH) port of the controller
D. Remote Authentication Dial-In User Service (RADIUS) token replay attack

Answer: B

NEW QUESTION 186
- (Exam Topic 15)
Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

A. Use Media Gateway Control Protocol (MGCP)
B. Use Transport Layer Security (TLS) protocol
C. Use File Transfer Protocol (FTP)
D. Use Secure Shell (SSH) protocol

Answer: B

NEW QUESTION 187
- (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 191
- (Exam Topic 15)
Which of the following vulnerability assessment activities BEST exemplifies the Examine method of assessment?

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

Answer: D

NEW QUESTION 194
- (Exam Topic 15)
Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

A. Training department
B. Internal audit
C. Human resources
D. Information technology (IT)

Answer: C

NEW QUESTION 198
- (Exam Topic 15)
Which of the following types of web-based attack is happening when an attacker is able to send a well-crafted, malicious request to an authenticated user without the user realizing it?

A. ross-Site Scripting (XSS)
B. Cross-Site request forgery (CSRF)
C. Cross injection
D. Broken Authentication And Session Management

Answer: B

NEW QUESTION 201
- (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 203

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

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

Answer: A

NEW QUESTION 206
- (Exam Topic 15)
A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

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

Answer: C

NEW QUESTION 209
- (Exam Topic 15)
What Is a risk of using commercial off-the-shelf (COTS) products?

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

Answer: A

NEW QUESTION 210
- (Exam Topic 15)
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

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

Answer: A

NEW QUESTION 213
- (Exam Topic 15)
A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

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

Answer: D

NEW QUESTION 214
- (Exam Topic 15)
Which of the following is a key responsibility for a data steward assigned to manage an enterprise data lake?

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

Answer: A

NEW QUESTION 216
- (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 218
- (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 220
- (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 225
- (Exam Topic 15)
Which of the following documents specifies services from the client's viewpoint?

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

Answer: C

NEW QUESTION 229
- (Exam Topic 15)
How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?

A. Access control can rely on the Operating System (OS), but eavesdropping is
B. Access control cannot rely on the Operating System (OS), and eavesdropping
C. Access control can rely on the Operating System (OS), and eavesdropping is
D. Access control cannot rely on the Operating System (OS), and eavesdropping

Answer: C

NEW QUESTION 231
- (Exam Topic 15)
In Identity Management (IdM), when is the verification stage performed?

A. As part of system sign-on
B. Before creation of the identity
C. After revocation of the identity
D. During authorization of the identity

Answer: A

NEW QUESTION 235
- (Exam Topic 15)
When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

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

Answer: B

NEW QUESTION 236
- (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 238
- (Exam Topic 15)
Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

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

Answer: C

NEW QUESTION 241
- (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 244
- (Exam Topic 15)
Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

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

Answer: A

NEW QUESTION 246
- (Exam Topic 15)
An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

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

Answer: B

NEW QUESTION 248
- (Exam Topic 15)
Which of the following BEST ensures the integrity of transactions to intended recipients?

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

Answer: A

NEW QUESTION 253
- (Exam Topic 15)
Which of the following is the BEST option to reduce the network attack surface of a system?

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

Answer: C

NEW QUESTION 254
- (Exam Topic 15)
An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data

protection methods.
Which of the following is the BEST data protection method?

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

Answer: C

NEW QUESTION 258
- (Exam Topic 15)
When performing an investigation with the potential for legal action, what should be the analyst's FIRST consideration?

A. Chain-of-custody
B. Authorization to collect
C. Court admissibility
D. Data decryption

Answer: A

NEW QUESTION 261
- (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 264
- (Exam Topic 15)
An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weal

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

Answer: A

NEW QUESTION 269
- (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 271
- (Exam Topic 15)
Which of the following vulnerabilities can be BEST detected using automated analysis?

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

Answer: D

NEW QUESTION 274
- (Exam Topic 15)
What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

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

Answer: D

NEW QUESTION 276
- (Exam Topic 15)
A company wants to store data related to users on an offsite server. What method can be deployed to protect the privacy of the user's information while maintaining the field-level configuration of the database?

A. {Encryption
B. Encoding
C. Tokenization
D. Hashing

Answer: A

NEW QUESTION 279
- (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 284
- (Exam Topic 15)
A hacker can use a lockout capability to start which of the following attacks?

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

Answer: A

NEW QUESTION 286
- (Exam Topic 15)
Which of the following is the MOST important consideration in selecting a security testing method based on different Radio-Frequency Identification (RFID) vulnerability types?

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

Answer: C

NEW QUESTION 287
- (Exam Topic 15)
In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

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

Answer: A

NEW QUESTION 288
- (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 291
- (Exam Topic 15)
Which of the following is the BEST method to gather evidence from a computer's hard drive?

A. Disk duplication
B. Disk replacement

C. Forensic signature
D. Forensic imaging

Answer: D

NEW QUESTION 296
- (Exam Topic 15)
Which of the following is the FIRST step during digital identity provisioning?

A. Authorizing the entity for resource access
B. Synchronizing directories
C. Issuing an initial random password
D. Creating the entity record with the correct attributes

Answer: D

NEW QUESTION 300
- (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 304
- (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 307
- (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 311
- (Exam Topic 15)
A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

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

Answer: D

NEW QUESTION 312
- (Exam Topic 15)
What is the FIRST step prior to executing a test of an organisation's disaster recovery (DR) or business continuity plan (BCP)?

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

Answer: D

NEW QUESTION 315
- (Exam Topic 15)
In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

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

Answer: D

NEW QUESTION 318
- (Exam Topic 15)
Which security feature fully encrypts code and data as it passes to the servers and only decrypts below the hypervisor layer?

A. File-system level encryption
B. Transport Layer Security (TLS)
C. Key management service
D. Trusted execution environments

Answer: D

NEW QUESTION 323
- (Exam Topic 15)
What is a security concern when considering implementing software-defined networking (SDN)?

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

Answer: C

NEW QUESTION 328
- (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 332
- (Exam Topic 15)
When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

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

Answer: A

NEW QUESTION 337
- (Exam Topic 15)
A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

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

Answer: C

NEW QUESTION 340
- (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 341
- (Exam Topic 15)
Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

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

Answer: B

NEW QUESTION 343
- (Exam Topic 15)
Which media sanitization methods should be used for data with a high security categorization?

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

Answer: D

NEW QUESTION 345
- (Exam Topic 15)
An information security professional is reviewing user access controls on a customer-facing application. The application must have multi-factor authentication (MFA) in place. The application currently requires a username and password to login. Which of the following options would BEST implement MFA?

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

Answer: C

NEW QUESTION 348
- (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 350
- (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 351
- (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 355
- (Exam Topic 15)
How is it possible to extract private keys securely stored on a cryptographic smartcard?

A. Bluebugging
B. Focused ion-beam
C. Bluejacking
D. Power analysis

Answer:

D

NEW QUESTION 357
- (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 358
- (Exam Topic 15)
The security architect has been mandated to assess the security of various brands of mobile devices. At what phase of the product lifecycle would this be MOST likely to occur?

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

Answer: C

NEW QUESTION 363
- (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 367
- (Exam Topic 15)
During testing, where are the requirements to inform parent organizations, law enforcement, and a computer incident response team documented?

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

Answer: D

NEW QUESTION 369
- (Exam Topic 15)
An application developer receives a report back from the security team showing their automated tools were able to successfully enter unexpected data into the organization's customer service portal, causing the site to crash. This is an example of which type of testing?

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

Answer: D

NEW QUESTION 372
- (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 377
- (Exam Topic 15)
Which of the following is a covert channel type?

A. Storage
B. Pipe

C. Memory
D. Monitoring

Answer: A

NEW QUESTION 378
- (Exam Topic 15)
Which of the following activities should a forensic examiner perform FIRST when determining the priority of digital evidence collection at a crime scene?

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

Answer: C

NEW QUESTION 382
- (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 387
- (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 392
- (Exam Topic 15)
In Federated Identity Management (FIM), which of the following represents the concept of federation?

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

Answer: D

NEW QUESTION 397
- (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 400
- (Exam Topic 15)
The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a
level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

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

Answer: D

NEW QUESTION 403
- (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 407
- (Exam Topic 15)
What is the BEST reason to include supply chain risks in a corporate risk register?

A. Risk registers help fund corporate supply chain risk management (SCRM) systems.
B. Risk registers classify and categorize risk and allow risks to be compared to corporate risk appetite.
C. Risk registers can be used to illustrate residual risk across the company.
D. Risk registers allow for the transfer of risk to third parties.

Answer: B

NEW QUESTION 408
- (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 413
- (Exam Topic 15)
How does Radio-Frequency Identification (RFID) assist with asset management?

A. It uses biometric information for system identification.
B. It uses two-factor authentication (2FA) for system identification.
C. It transmits unique Media Access Control (MAC) addresses wirelessly.
D. It transmits unique serial numbers wirelessly.

Answer: B

NEW QUESTION 415
- (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 416
- (Exam Topic 15)
Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

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

Answer: A

NEW QUESTION 418
- (Exam Topic 15)
In an IDEAL encryption system, who has sole access to the decryption key?

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

Answer:

B

NEW QUESTION 419
- (Exam Topic 15)
The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

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

Answer: A

NEW QUESTION 420
- (Exam Topic 14)
What is the MOST effective way to determine a mission critical asset in an organization?

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

Answer: B

NEW QUESTION 421
- (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 424
- (Exam Topic 14)
What form of attack could this represent?

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

Answer: D

NEW QUESTION 429
- (Exam Topic 14)
Which of the following are core categories of malicious attack against Internet of Things (IOT) devices?

A. Packet capture and false data injection
B. Packet capture and brute force attack
C. Node capture 3nd Structured Query Langue (SQL) injection
D. Node capture and false data injection

Answer: D

NEW QUESTION 434
- (Exam Topic 14)
In a dispersed network that lacks central control, which of the following is die PRIMARY course of action to mitigate exposure?

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

Answer: C

NEW QUESTION 435
- (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 440
- (Exam Topic 14)
Continuity of operations is BEST supported by which of the following?

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

Answer: B

NEW QUESTION 443
- (Exam Topic 14)
Which of the following is the PRIMARY risk associated with Extensible Markup Language (XML) applications?

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

Answer: A

NEW QUESTION 446
- (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 451
- (Exam Topic 14)
If a content management system (CMC) is implemented, which one of the following would occur?

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

Answer: D

NEW QUESTION 452
- (Exam Topic 14)
What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

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

Answer: D

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

NEW QUESTION 456
- (Exam Topic 14)
A large corporation is looking for a solution to automate access based on where the request is coming from, who the user is, what device they are connecting with, and what and time of day they are attempting this access. What type of solution would suit their needs?

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

Answer: B

NEW QUESTION 458
- (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 459
- (Exam Topic 14)

A. Verify the camera's log for recent logins outside of the Internet Technology (IT) department.
B. Verify the security and encryption protocol the camera uses.
C. Verify the security camera requires authentication to log into the management console.
D. Verify the most recent firmware version is installed on the camera.

Answer: D

NEW QUESTION 463
- (Exam Topic 14)
What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

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

Answer: B

NEW QUESTION 468
- (Exam Topic 14)
What are the roles within a scrum methodology?

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

Answer: D

NEW QUESTION 471
- (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 473
- (Exam Topic 14)
Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

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

Answer: C

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

NEW QUESTION 476
- (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 478
- (Exam Topic 14)
Which of the following is a characteristic of convert security testing?

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

Answer: B

NEW QUESTION 482
- (Exam Topic 14)
Which of the following is a method of attacking internet (IP) v6 Layer 3 and Layer 4 ?

A. Synchronize sequence numbers (SVN) flooding
B. Internet Control Message Protocol (IOP) flooring
C. Domain Name Server [DNS) cache poisoning
D. Media Access Control (MAC) flooding

Answer: A

NEW QUESTION 486
- (Exam Topic 14)
Which of the following is the MOST important reason for using a chain of custody from?

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

Answer: A

NEW QUESTION 490
- (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 492
- (Exam Topic 14)
Limiting the processor, memory, and Input/output (I/O) capabilities of mobile code is known as

A. code restriction.
B. on-demand compile.
C. sandboxing.
D. compartmentalization.

Answer: C

NEW QUESTION 497
- (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 500
- (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 503
- (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 506
- (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 511
- (Exam Topic 14)
When selecting a disk encryption technology, which of the following MUST also be assured to be encrypted?

A. Master Boot Record (MBR)
B. Pre-boot environment
C. Basic Input Output System (BIOS)
D. Hibernation file

Answer: A

NEW QUESTION 512
- (Exam Topic 14)
Which of the following is the final phase of the identity and access provisioning lifecycle?

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

Answer: B

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

NEW QUESTION 513
- (Exam Topic 14)
Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

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

Answer: B

NEW QUESTION 518
- (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 521

- (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 522
- (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 524
- (Exam Topic 14)
If a content management system (CSM) is implemented, which one of the following would occur?

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

Answer: A

NEW QUESTION 528
- (Exam Topic 14)
Which layer of the Open system Interconnect (OSI) model is responsible for secure data transfer between applications, flow control, and error detection and correction?

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

Answer: B

NEW QUESTION 531
- (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 536
- (Exam Topic 14)
In order for application developers to detect potential vulnerabilities earlier during the Software Development Life Cycle (SDLC), which of the following safeguards should be implemented FIRST as part of a comprehensive testing framework?

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

Answer: A

NEW QUESTION 539
- (Exam Topic 14)
Which of the following job functions MUST be separated to maintain data and application integrity?

A. Applications development and systems analysis
B. Production control and data control functions

C. Scheduling and computer operations
D. Systems development and systems maintenance

Answer: D

NEW QUESTION 542
- (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 544
- (Exam Topic 14)
Which of the following open source software issues pose the MOST risk to an application?

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

Answer: D

NEW QUESTION 546
- (Exam Topic 14)
What is the MOST effective way to protect privacy?

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

Answer: D

NEW QUESTION 549
- (Exam Topic 14)
The core component of Role Based Access control (RBAC) must be constructed of defined data elements. Which elements are required?

A. Users, permissions, operators, and protected objects
B. Users, rotes, operations, and protected objects
C. Roles, accounts, permissions, and protected objects
D. Roles, operations, accounts, and protected objects

Answer: B

NEW QUESTION 552
- (Exam Topic 14)
An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.
Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

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

Answer: A

NEW QUESTION 554
- (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 558
- (Exam Topic 14)

Which of the following would an internal technical security audit BEST validate?

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

Answer: D

NEW QUESTION 562
- (Exam Topic 14)
Which layer of the Open systems Interconnection (OSI) model is being targeted in the event of a Synchronization (SYN) flood attack?

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

Answer: B

NEW QUESTION 564
- (Exam Topic 14)
Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

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

Answer: C

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

NEW QUESTION 566
- (Exam Topic 14)
Which of the following needs to be included in order for High Availability (HA) to continue operations during planned system outages?

A. Redundant hardware, disk spanning, and patching
B. Load balancing, power reserves, and disk spanning
C. Backups, clustering, and power reserves
D. Clustering, load balancing, and fault-tolerant options

Answer: D

NEW QUESTION 569
- (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 573
- (Exam Topic 14)
Which of the following is a PRIMARY challenge when running a penetration test?

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

Answer: D

NEW QUESTION 578
- (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 582
- (Exam Topic 14)
Which of the following initiates the systems recovery phase of a disaster recovery plan?

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

Answer: A

NEW QUESTION 586
- (Exam Topic 14)
What is the BEST way to correlate large volumes of disparate data sources in a Security Operations Center (SOC) environment?

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

Answer: B

NEW QUESTION 589
- (Exam Topic 14)
When deploying en Intrusion Detection System (IDS) on a high-volume network, the need to distribute the load across multiple sensors would create which technical problem?

A. Session continuity
B. Proxy authentication failure
C. Sensor overload
D. Synchronized sensor updates

Answer: A

NEW QUESTION 591
- (Exam Topic 14)
Which of the following authorization standards is built to handle Application programming Interface (API) access for federated Identity management (FIM)?

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

Answer: C

NEW QUESTION 594
- (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 598
- (Exam Topic 14)
When using Security Assertion markup language (SAML), it is assumed that the principal subject

A. accepts persistent cookies from the system.
B. allows Secure Sockets Layer (SSL) for data exchanges.
C. is on a system that supports remote authorization.
D. enrolls with at least one identity provider.

Answer: D

NEW QUESTION 602
- (Exam Topic 14)
Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device Which has stolen?

A. Whole device encryption with key escrow
B. Mobile Device Management (MDMJ with device wipe

C. Mobile device tracking with geolocation
D. Virtual Private Network (VPN) with traffic encryption

Answer: B

NEW QUESTION 606
- (Exam Topic 14)
Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for implementing network security?

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

Answer: C

NEW QUESTION 608
- (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 610
- (Exam Topic 14)
An analysis finds unusual activity coming from a computer that was thrown away several months prior, which of the following steps ensure the proper removal of the system?

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

Answer: B

NEW QUESTION 613
- (Exam Topic 14)
Which is the MOST effective countermeasure to prevent electromagnetic emanations on unshielded data cable?

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

Answer: B

NEW QUESTION 614
- (Exam Topic 14)
Which of the following media is least problematic with data remanence?

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

Answer: C

NEW QUESTION 618
- (Exam Topic 14)
What is the best way for mutual authentication of devices belonging to the same organization?

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

Answer: A

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

NEW QUESTION 621
- (Exam Topic 14)
During a recent assessment an organization has discovered that the wireless signal can be detected outside the campus area. What logical control should be implemented in order to BFST protect One confidentiality of information traveling One wireless transmission media?

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

Answer: B

NEW QUESTION 624
- (Exam Topic 14)
Change management policies and procedures belong to which of the following types of controls?

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

Answer: A

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

NEW QUESTION 625
- (Exam Topic 14)
Which of the following is the MOST important action regarding authentication?

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

Answer: B

NEW QUESTION 628
- (Exam Topic 14)
An audit of an application reveals that the current configuration does not match the configuration of the originally implemented application. Which of the following is the FIRST action to be taken?

A. Recommend an update to the change control process.
B. Verify the approval of the configuration change.
C. Roll back the application to the original configuration.
D. Document the changes to the configuration.

Answer: B

NEW QUESTION 633
- (Exam Topic 14)
A security professional recommends that a company integrate threat modeling into its Agile development processes. Which of the following BEST describes the benefits of this approach?

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

Answer: D

NEW QUESTION 638
- (Exam Topic 14)
What high Availability (HA) option of database allows multiple clients to access multiple database servers simultaneously?

A. Non-Structured Query Language (NoSQL) database
B. Relational database
C. Shadow database
D. Replicated database

Answer: C

NEW QUESTION 641
- (Exam Topic 14)
The adoption of an enterprise-wide business continuity program requires Which of the following?

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

Answer: D

NEW QUESTION 646
- (Exam Topic 14)
Which of the following is the BEST way to protect against structured Query language (SQL) injection?

A. Enforce boundary checking.
B. Restrict use of SELECT command.
C. Restrict Hyper Text Markup Language (HTNL) source code access.
D. Use stored procedures.

Answer: D

NEW QUESTION 649
- (Exam Topic 14)
Which of the following is true of Service Organization Control (SOC) reports?

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

Answer: B

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

NEW QUESTION 652
- (Exam Topic 14)
An Intrusion Detection System (IDS) is based on the general hypothesis that a security violation is associated with a pattern of system usage which can be

A. differentiated from a normal usage pattern.
B. used to detect known violations.
C. used to detect a masquerader.
D. differentiated to detect all security violations.

Answer: A

NEW QUESTION 654
- (Exam Topic 14)
Which of the following is the MOST significant benefit to implementing a third-party federated identity architecture?

A. Attribute assertions as agencies can request a larger set of attributes to fulfill service delivery
B. Data decrease related to storing personal information
C. Reduction in operational costs to the agency
D. Enable business objectives so departments can focus on mission rather than the business of identitymanagement

Answer: C

NEW QUESTION 658
- (Exam Topic 14)
Which of the following will help prevent improper session handling?

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

Answer: B

NEW QUESTION 661
- (Exam Topic 14)
How does identity as a service (IDaaS) provide an easy mechanism for integrating identity service into individual applications with minimal development effort?

A. By allowing the identification logic and storage of an identity's attributes to be maintained externally
B. By integrating internal provisioning procedures with external authentication processes
C. By allowing for internal provisioning of user accounts
D. By keeping all user information in easily accessible cloud repositories

Answer: D

NEW QUESTION 665
- (Exam Topic 14)
Why might a network administrator choose distributed virtual switches instead of stand-alone switches for network segmentation?

A. To standardize on a single vendor
B. To ensure isolation of management traffic
C. To maximize data plane efficiency
D. To reduce the risk of configuration errors

Answer: C

NEW QUESTION 668
- (Exam Topic 14)
A security consultant has been hired by a company to establish its vulnerability management program. The consultant is now in the deployment phase. Which of the following tasks is part of this process?

A. Select and procure supporting technologies.
B. Determine a budget and cost analysis for the program.
C. Measure effectiveness of the program’s stated goals.
D. Educate and train key stakeholders.

Answer: C

NEW QUESTION 670
- (Exam Topic 14)
Which of the following should be included in a hardware retention policy? Which of the following should be included in a hardware retention policy?

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

Answer: A

NEW QUESTION 672
- (Exam Topic 14)
Which of the following needs to be taken into account when assessing vulnerability?

A. Risk identification and validation
B. Threat mapping
C. Risk acceptance criteria
D. Safeguard selection

Answer: A

Explanation:
Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA478&lpg=PA478&dq=CISSP+taken+into+acc

NEW QUESTION 677
- (Exam Topic 14)
An Internet software application requires authentication before a user is permitted to utilize the resource. Which testing scenario BEST validates the functionality of the application?

A. Reasonable data testing
B. Input validation testing
C. Web session testing
D. Allowed data bounds and limits testing

Answer: B

NEW QUESTION 681
- (Exam Topic 14)
Which programming methodology allows a programmer to use pre-determined blocks of code end consequently reducing development time and programming costs?

A. Application security
B. Object oriented
C. Blocked algorithm
D. Assembly language

Answer: B

NEW QUESTION 683
- (Exam Topic 14)

What technique used for spoofing the origin of an email can successfully conceal the sender s Internet Protocol (IP) address?

A. Change In-Reply-To data
B. Web crawling
C. Onion routing
D. Virtual Private Network (VPN)

Answer: C

NEW QUESTION 685
- (Exam Topic 14)
Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

A. Ensures that there is no loss of functionality between releases
B. Allows for future enhancements to existing features
C. Enforces backward compatibility between releases
D. Ensures that a trace for all deliverables is maintained and auditable

Answer: C

NEW QUESTION 686
- (Exam Topic 14)
Which attack defines a piece of code that is inserted into software to trigger a malicious function?

A. Phishing
B. Salami
C. Back door
D. Logic bomb

Answer: D

NEW QUESTION 690
- (Exam Topic 14)

A. The signer verifies that the software being loaded is the software originated by the signer.
B. The vendor certifies the software being loaded is free of malicious code and that it was originated by the signer.
C. The signer verifies that the software being loaded is free of malicious code.
D. Both vendor and the signer certify the software being loaded is free of malicious code and it was originated by the signer.

Answer: A

NEW QUESTION 693
- (Exam Topic 14)
Which of the following actions MUST be performed when using secure multipurpose internet mail Extension (S/MIME) before sending an encrypted message to a recipient?

A. Digitally sign foe message.
B. Obtain the recipients private key.
C. Obtain the recipient's digital certificate.
D. Encrypt attachments.

Answer: A

NEW QUESTION 695
- (Exam Topic 14)
Which of the following presents the PRIMARY concern to an organization when setting up a federated single sign-on (SSO) solution with another

A. Sending assertions to an identity provider
B. Requesting Identity assertions from the partners domain
C. defining the identity mapping scheme
D. Having the resource provider query the Identity provider

Answer: C

NEW QUESTION 700
- (Exam Topic 14)
Which of the following is a characteristic of a challenge/response authentication process?

A. Using a password history blacklist
B. Transmitting a hash based on the user's password
C. Presenting distorted gravies of text for authentication
D. Requiring the use of non-consecutive numeric characters

Answer: C

NEW QUESTION 705

- (Exam Topic 14)
In the common criteria (CC) for information technology (IT) security evaluation, increasing Evaluation Assurance Levels (EAL) results in which of the following?

A. Increased functionality
B. Increased interoperability
C. Increase in resource requirement
D. Increase in evaluated systems

Answer: B

NEW QUESTION 709
- (Exam Topic 14)
Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

A. Watering hole
B. Brute force
C. Spear phishing
D. Address Resolution Protocol (ARP) poisoning

Answer: D

NEW QUESTION 713
- (Exam Topic 14)
A security professional should consider the protection of which of the following elements FIRST when developing a defense-in-depth strategy for a mobile workforce?

A. Network perimeters
B. Demilitarized Zones (DM2)
C. Databases and back-end servers
D. End-user devices

Answer: D

NEW QUESTION 715
- (Exam Topic 14)
A large corporation is locking for a solution to automate access based on where on request is coming from, who the user is, what device they are connecting with, and what time of day they are attempting this access. What type of solution would suit their needs?

A. Discretionary Access Control (DAC)
B. Role Based Access Control (RBAC)
C. Mandater Access Control (MAC)
D. Network Access Control (NAC)

Answer: D

NEW QUESTION 717
- (Exam Topic 14)
Which of the following is critical if an empolyee is dismissed due to violation of an organization’s acceptable use policy (Aup) ?

A. Appropriate documentation
B. privilege suspension
C. proxy records
D. Internet access logs

Answer: A

NEW QUESTION 720
- (Exam Topic 14)
As a security manger which of the following is the MOST effective practice for providing value to an organization?

A. Assess business risk and apply security resources accordingly
B. Coordinate security implementations with internal audit
C. Achieve compliance regardless of related technical issues
D. Identify confidential information and protect it

Answer: D

NEW QUESTION 722
- (Exam Topic 14)
Which of the following is the weakest form of protection for an application that handles Personally Identifiable Information (PII)?

A. Transport Layer Security (TLS)
B. Ron Rivest Cipher 4 (RC4) encryption
C. Security Assertion Markup Language (SAML)
D. Multifactor authentication

Answer: B

NEW QUESTION 724
- (Exam Topic 14)
What does the term “100-year floodplain” mean to emergency preparedness officials?

A. The area is expected to be safe from flooding for at least 100 years.
B. The odds of a flood at this level are 1 in 100 in any given year.
C. The odds are that the next significant flood will hit within the next 100 years.
D. The last flood of any kind to hit the area was more than 100 years ago.

Answer: B

NEW QUESTION 729
- (Exam Topic 13)
From a security perspective, which of the following assumptions MUST be made about input to an application?

A. It is tested
B. It is logged
C. It is verified
D. It is untrusted

Answer: D

NEW QUESTION 733
- (Exam Topic 14)
Individuals have been identified and determined as having a need-to-know for the information. Which of the following access control methods MUST include a consistent set of rules for controlling and limiting access?

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

Answer: D

NEW QUESTION 734
- (Exam Topic 13)
Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

A. Large mantrap where groups of individuals leaving are identified using facial recognition technology
B. Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exitdoor
C. Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list
D. Card-activated turnstile where individuals are validated upon exit

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 737
- (Exam Topic 13)
A security analyst for a large financial institution is reviewing network traffic related to an incident. The analyst determines the traffic is irrelevant to the investigation but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user’s desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst’s next step?

A. Send the log file co-workers for peer review
B. Include the full network traffic logs in the incident report
C. Follow organizational processes to alert the proper teams to address the issue.
D. Ignore data as it is outside the scope of the investigation and the analyst’s role.

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 741
- (Exam Topic 13)
What is the PRIMARY role of a scrum master in agile development?

A. To choose the primary development language
B. To choose the integrated development environment
C. To match the software requirements to the delivery plan
D. To project manage the software delivery

Answer: D

NEW QUESTION 743
- (Exam Topic 13)
A minimal implementation of endpoint security includes which of the following?

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

Answer: B

NEW QUESTION 748
- (Exam Topic 13)
Which of the following access management procedures would minimize the possibility of an organization's employees retaining access to secure werk areas after they change roles?

A. User access modification
B. user access recertification
C. User access termination
D. User access provisioning

Answer: B

NEW QUESTION 752
- (Exam Topic 13)
Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 757
- (Exam Topic 13)
Which of the following is part of a Trusted Platform Module (TPM)?

A. A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion
B. A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for “measuring”the state of a computing platform
C. A secure processor targeted at managing digital keys and accelerating digital signing
D. A platform-independent software interface for accessing computer functions

Answer: A

NEW QUESTION 759
- (Exam Topic 13)
Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

A. Application proxy
B. Port filter
C. Network boundary router
D. Access layer switch

Answer: D

NEW QUESTION 764
- (Exam Topic 13)
Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

A. undergo a security assessment as part of authorization process
B. establish a risk management strategy
C. harden the hosting server, and perform hosting and application vulnerability scans
D. establish policies and procedures on system and services acquisition

Answer: D

NEW QUESTION 767
- (Exam Topic 13)
Which of the following MUST be in place to recognize a system attack?

A. Stateful firewall
B. Distributed antivirus
C. Log analysis
D. Passive honeypot

Answer:

C

NEW QUESTION 771
- (Exam Topic 13)
Which of the following is the MOST effective method to mitigate Cross-Site Scripting (XSS) attacks?

A. Use Software as a Service (SaaS)
B. Whitelist input validation
C. Require client certificates
D. Validate data output

Answer: B

NEW QUESTION 775
- (Exam Topic 13)
An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies.
What code of ethics canon is being observed?

A. Provide diligent and competent service to principals
B. Protect society, the commonwealth, and the infrastructure
C. Advance and protect the profession
D. Act honorable, honesty, justly, responsibly, and legally

Answer: A

Explanation:
Section: Security Operations

NEW QUESTION 779
- (Exam Topic 13)
Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

A. Code quality, security, and origin
B. Architecture, hardware, and firmware
C. Data quality, provenance, and scaling
D. Distributed, agile, and bench testing

Answer: A

NEW QUESTION 782
- (Exam Topic 13)
As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?

A. Known-plaintext attack
B. Denial of Service (DoS)
C. Cookie manipulation
D. Structured Query Language (SQL) injection

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 785
- (Exam Topic 13)
Which of the following is a responsibility of a data steward?

A. Ensure alignment of the data governance effort to the organization.
B. Conduct data governance interviews with the organization.
C. Document data governance requirements.
D. Ensure that data decisions and impacts are communicated to the organization.

Answer: A

NEW QUESTION 789
- (Exam Topic 13)
Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

A. Truncating parts of the data
B. Applying Access Control Lists (ACL) to the data
C. Appending non-watermarked data to watermarked data
D. Storing the data in a database

Answer: A

NEW QUESTION 792
- (Exam Topic 13)
What is the MAIN goal of information security awareness and training?

A. To inform users of the latest malware threats
B. To inform users of information assurance responsibilities
C. To comply with the organization information security policy
D. To prepare students for certification

Answer: B

NEW QUESTION 793
- (Exam Topic 13)
Which of the following is a responsibility of the information owner?

A. Ensure that users and personnel complete the required security training to access the Information System (IS)
B. Defining proper access to the Information System (IS), including privileges or access rights
C. Managing identification, implementation, and assessment of common security controls
D. Ensuring the Information System (IS) is operated according to agreed upon security requirements

Answer: C

NEW QUESTION 797
- (Exam Topic 13)
A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results. What should be implemented to BEST achieve the desired results?

A. Configuration Management Database (CMDB)
B. Source code repository
C. Configuration Management Plan (CMP)
D. System performance monitoring application

Answer: A

NEW QUESTION 798
- (Exam Topic 13)
The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. Which elements are required?

A. Users, permissions, operations, and protected objects
B. Roles, accounts, permissions, and protected objects
C. Users, roles, operations, and protected objects
D. Roles, operations, accounts, and protected objects

Answer: C

NEW QUESTION 803
- (Exam Topic 13)
Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

A. Acoustic sensor
B. Motion sensor
C. Shock sensor
D. Photoelectric sensor

Answer: C

NEW QUESTION 804
- (Exam Topic 13)
Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

A. Senior management
B. Information security department
C. Audit committee
D. All users

Answer: C

NEW QUESTION 809
- (Exam Topic 13)
Which of the following mechanisms will BEST prevent a Cross-Site Request Forgery (CSRF) attack?

A. parameterized database queries
B. whitelist input values
C. synchronized session tokens
D. use strong ciphers

Answer:

C

NEW QUESTION 813
- (Exam Topic 13)
Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

A. Increased console lockout times for failed logon attempts
B. Reduce the group in size
C. A credential check-out process for a per-use basis
D. Full logging on affected systems

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 816
- (Exam Topic 13)
Which of the BEST internationally recognized standard for evaluating security products and systems?

A. Payment Card Industry Data Security Standards (PCI-DSS)
B. Common Criteria (CC)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Sarbanes-Oxley (SOX)

Answer: B

NEW QUESTION 819
- (Exam Topic 13)
What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

A. Non-repudiation
B. Efficiency
C. Confidentially
D. Privacy

Answer: A

NEW QUESTION 820
- (Exam Topic 13)
Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

A. Minimize malicious attacks from third parties
B. Manage resource privileges
C. Share digital identities in hybrid cloud
D. Defined a standard protocol

Answer: B

NEW QUESTION 824
- (Exam Topic 13)
An organization plan on purchasing a custom software product developed by a small vendor to support its business model. Which unique consideration should be made part of the contractual agreement potential
long-term risks associated with creating this dependency?

A. A source code escrow clause
B. Right to request an independent review of the software source code
C. Due diligence form requesting statements of compliance with security requirements
D. Access to the technical documentation

Answer: B

NEW QUESTION 825
- (Exam Topic 13)
Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

Answer: A

NEW QUESTION 829
- (Exam Topic 13)
It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

A. Negotiate schedule with the Information Technology (IT) operation’s team
B. Log vulnerability summary reports to a secured server
C. Enable scanning during off-peak hours
D. Establish access for Information Technology (IT) management

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 830
- (Exam Topic 13)
A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

A. Put the device in airplane mode
B. Suspend the account with the telecommunication provider
C. Remove the SIM card
D. Turn the device off

Answer: A

NEW QUESTION 832
- (Exam Topic 13)
When conducting a security assessment of access controls, which activity is part of the data analysis phase?

A. Present solutions to address audit exceptions.
B. Conduct statistical sampling of data transactions.
C. Categorize and identify evidence gathered during the audit.
D. Collect logs and reports.

Answer: C

NEW QUESTION 837
- (Exam Topic 12)
During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

A. Calculate the value of assets being accredited.
B. Create a list to include in the Security Assessment and Authorization package.
C. Identify obsolete hardware and software.
D. Define the boundaries of the information system.

Answer: A

NEW QUESTION 842
- (Exam Topic 12)
In which identity management process is the subject’s identity established?

A. Trust
B. Provisioning
C. Authorization
D. Enrollment

Answer: D

NEW QUESTION 846
- (Exam Topic 12)
Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A. It must be known to both sender and receiver.
B. It can be transmitted in the clear as a random number.
C. It must be retained until the last block is transmitted.
D. It can be used to encrypt and decrypt information.

Answer: B

NEW QUESTION 849
......