ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 15)
In addition to life, protection of which of the following elements is MOST important when planning a data center site?

A. Data and hardware
B. Property and operations
C. Profits and assets
D. Resources and reputation

Answer: D

NEW QUESTION 3
- (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 4
- (Exam Topic 15)
In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

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

Answer: C

NEW QUESTION 5
- (Exam Topic 15)
Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

A. Group Policy Object (GPO)
B. Network Access Control (NAC)
C. Mobile Device Management (MDM)
D. Privileged Access Management (PAM)

Answer: B

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

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

Answer: A

NEW QUESTION 7
- (Exam Topic 15)
A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

A. Service accounts removal
B. Data validation

C. Logging and monitoring
D. Data sanitization

Answer: B

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

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

Answer: D

NEW QUESTION 9
- (Exam Topic 15)
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 10
- (Exam Topic 15)
Which of the following routing protocols is used to exchange route information between public autonomous systems?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 15)
A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the
BEST design approach to securing this environment?

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

Answer: B

NEW QUESTION 14
- (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 18
- (Exam Topic 15)
Which of the following provides the MOST secure method for Network Access Control (NAC)?

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

Answer: B

NEW QUESTION 23

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

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

Answer: A

NEW QUESTION 27
- (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 31
- (Exam Topic 15)
Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

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

Answer: A

NEW QUESTION 35
- (Exam Topic 15)
What is the FIRST step for an organization to take before allowing personnel to access social media from a corporate device or user account?

A. Publish a social media guidelines document.
B. Publish an acceptable usage policy.
C. Document a procedure for accessing social media sites.
D. Deliver security awareness training.

Answer: A

NEW QUESTION 38
- (Exam Topic 15)
What is the P R IM A R Y reason criminal law is difficult to enforce when dealing with cyber-crime?

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

Answer: D

NEW QUESTION 39
- (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 40
- (Exam Topic 15)
Which of the following is the MOST effective method of detecting vulnerabilities in web-based applications early in the secure Software Development Life Cycle (SDLC)?

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

Answer: C

NEW QUESTION 44
- (Exam Topic 15)
Which of the following statements BEST distinguishes a stateful packet inspection firewall from a stateless packet filter firewall?

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

Answer: B

NEW QUESTION 45
- (Exam Topic 15)
Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

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

Answer: D

NEW QUESTION 49
- (Exam Topic 15)
In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

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

Answer: B

NEW QUESTION 52
- (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 57
- (Exam Topic 15)
Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

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

Answer: C

NEW QUESTION 58
- (Exam Topic 15)
Which of the following is the BEST way to mitigate circumvention of access controls?

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

Answer: D

NEW QUESTION 62
- (Exam Topic 15)
What type of investigation applies when malicious behavior is suspected between two organizations?

A. Regulatory
B. Criminal
C. Civil
D. Operational

Answer:

A

NEW QUESTION 67
- (Exam Topic 15)
Which element of software supply chain management has the GREATEST security risk to organizations?

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

Answer: B

NEW QUESTION 71
- (Exam Topic 15)
Who should formulate conclusions from a particular digital fore Ball, Submit a Toper Of Tags, and the results?

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

Answer: B

NEW QUESTION 73
- (Exam Topic 15)
A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

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

Answer: D

NEW QUESTION 78
- (Exam Topic 15)
As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem?

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

Answer: C

NEW QUESTION 79
- (Exam Topic 15)

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

Answer: D

NEW QUESTION 83
- (Exam Topic 15)
Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

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

Answer: B

NEW QUESTION 88
- (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 90
- (Exam Topic 15)
When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

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

Answer: C

NEW QUESTION 94
- (Exam Topic 15)
Which of the following is the MOST common cause of system or security failures?

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

Answer: D

NEW QUESTION 98
- (Exam Topic 15)
Which of the following are mandatory canons for the (ISC)* Code of Ethics?

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

Answer: D

NEW QUESTION 101
- (Exam Topic 15)
Which of the following is MOST important to follow when developing information security controls for an organization?

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

Answer: C

NEW QUESTION 103
- (Exam Topic 15)
An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

A. Data driven risk assessment with a focus on data
B. Security controls driven assessment that focuses on controls management
C. Business processes based risk assessment with a focus on business goals
D. Asset driven risk assessment with a focus on the assets

Answer: A

NEW QUESTION 106
- (Exam Topic 15)
In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below.
Which of the following would be a reasonable annual loss expectation?

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

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

Answer: B

NEW QUESTION 111
- (Exam Topic 15)
A client server infrastructure that provides user-to-server authentication describes which one of the following?

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

Answer: B

NEW QUESTION 116
- (Exam Topic 15)
In which of the following system life cycle processes should security requirements be developed?

A. Risk management
B. Business analysis
C. Information management
D. System analysis

Answer: B

NEW QUESTION 117
- (Exam Topic 15)
An application is used for funds transfer between an organization and a third-party. During a security audit, an issue with the business continuity/disaster recovery policy and procedures for this application. Which of the following reports should the audit file with the organization?

A. Service Organization Control (SOC) 1
B. Statement on Auditing Standards (SAS) 70
C. Service Organization Control (SOC) 2
D. Statement on Auditing Standards (SAS) 70-1

Answer: C

NEW QUESTION 122
- (Exam Topic 15)
Which of the following is the MOST effective countermeasure against data remanence?

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

Answer: A

NEW QUESTION 127
- (Exam Topic 15)
What is the BEST way to restrict access to a file system on computing systems?

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

Answer: C

NEW QUESTION 130
- (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 134

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

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

Answer: B

NEW QUESTION 135
- (Exam Topic 15)
Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

A. For the establishment, exercise, or defense of legal claims
B. The personal data has been lawfully processed and collected
C. The personal data remains necessary to the purpose for which it was collected
D. For the reasons of private interest

Answer: C

NEW QUESTION 136
- (Exam Topic 15)

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

Answer: D

NEW QUESTION 139
- (Exam Topic 15)
An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

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

Answer: D

NEW QUESTION 141
- (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 143
- (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 144
- (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 148
- (Exam Topic 15)
If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), which of the following becomes even MORE essential to the assurance of network?

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

Answer: C

NEW QUESTION 151
- (Exam Topic 15)
Before implementing an internet-facing router, a network administrator ensures that the equipment is baselined/hardened according to approved configurations and settings. This action provides protection against which of the following attacks?

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

Answer: B

NEW QUESTION 156
- (Exam Topic 15)
Using Address Space Layout Randomization (ASLR) reduces the potential for which of the following attacks?

A. SQL injection (SQLi)
B. Man-in-the-middle (MITM)
C. Cross-Site Scripting (XSS)
D. Heap overflow

Answer: D

NEW QUESTION 157
- (Exam Topic 15)
When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

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

Answer: C

NEW QUESTION 159
- (Exam Topic 15)
When assessing the audit capability of an application, which of the following activities is MOST important?

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

Answer: C

NEW QUESTION 160
- (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 161
- (Exam Topic 15)
Which of the following will accomplish Multi-Factor Authentication (MFA)?

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

Answer: A

NEW QUESTION 165
- (Exam Topic 15)
An organization has discovered that organizational data is posted by employees to data storage accessible to the general public. What is the PRIMARY step an organization must take
to ensure data is properly protected from public release?

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

Answer: C

NEW QUESTION 170
- (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 173
- (Exam Topic 15)
What is static analysis intended to do when analyzing an executable file?

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

Answer: D

NEW QUESTION 176
- (Exam Topic 15)
A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

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

Answer: C

NEW QUESTION 177
- (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 179
- (Exam Topic 15)
What is the benefit of using Network Admission Control (NAC)?

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

Answer: C

NEW QUESTION 182
- (Exam Topic 15)
Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

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

Answer: C

NEW QUESTION 185
- (Exam Topic 15)
Which of the following describes the order in which a digital forensic process is usually conducted?

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

Answer: A

NEW QUESTION 190
- (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 192
- (Exam Topic 15)
Which of the following is the PRIMARY purpose of due diligence when an organization embarks on a merger or acquisition?

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

Answer: A

NEW QUESTION 195
- (Exam Topic 15)
In a large company, a system administrator needs to assign users access to files using Role Based Access Control (RBAC). Which option Is an example of RBAC?

A. Mowing users access to files based on their group membership
B. Allowing users access to files based on username
C. Allowing users access to files based on the users location at time of access
D. Allowing users access to files based on the file type

Answer: A

NEW QUESTION 199
- (Exam Topic 15)
What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

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

Answer: C

NEW QUESTION 203
- (Exam Topic 15)
Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this TAM action?

A. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to services.

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

Answer: A

NEW QUESTION 207
- (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 212
- (Exam Topic 15)
Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

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

Answer: D

NEW QUESTION 214
- (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 218
- (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 221
- (Exam Topic 15)
When defining a set of security controls to mitigate a risk, which of the following actions MUST occur?

A. Each control's effectiveness must be evaluated individually.
B. Each control must completely mitigate the risk.
C. The control set must adequately mitigate the risk.
D. The control set must evenly divided the risk.

Answer: A

NEW QUESTION 222
- (Exam Topic 15)
Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

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

Answer: B

NEW QUESTION 223
- (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 226
- (Exam Topic 15)
An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

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

Answer: B

NEW QUESTION 228
- (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 231
- (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 235
- (Exam Topic 15)
The ability to send malicious code, generally in the form of a client side script, to a different end user is categorized as which type of vulnerability?

A. Session hijacking
B. Cross-site request forgery (CSRF)
C. Cross-Site Scripting (XSS)
D. Command injection

Answer: C

NEW QUESTION 239
- (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 244
- (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 249
- (Exam Topic 15)
Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

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

Answer: D

NEW QUESTION 253
- (Exam Topic 15)
Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

A. Multiprotocol Label Switching (MPLS)
B. Synchronous Optical Networking (SONET)
C. Session Initiation Protocol (SIP)
D. Fiber Channel Over Ethernet (FCoE)

Answer: A

NEW QUESTION 257
- (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 259
- (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 261
- (Exam Topic 15)
Which of the following explains why classifying data is an important step in performing a Risk assessment?

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

Answer: D

NEW QUESTION 263
- (Exam Topic 15)
An organization's internal audit team performed a security audit on the company's system and reported that the manufacturing application is rarely updated along with other issues categorized as minor. Six months later, an external audit team reviewed the same system with the same scope, but identified severe weaknesses in the manufacturing application's security controls. What is MOST likely to be the root cause of the internal audit team's failure in detecting these security issues?

A. Inadequate test coverage analysis
B. Inadequate security patch testing
C. Inadequate log reviews
D. Inadequate change control procedures

Answer: A

NEW QUESTION 265

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

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

Answer: A

NEW QUESTION 266
- (Exam Topic 15)
The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

A. Removal of service accounts from review
B. Segregation of Duties (SoD)
C. Clear provisioning policies
D. Frequent audits

Answer: C

NEW QUESTION 268
- (Exam Topic 15)
The Open Web Application Security Project’s (OWASP) Software Assurance Maturity Model (SAMM) allows organizations to implement a flexible software security strategy to measure organizational impact based on what risk management aspect?

A. Risk tolerance
B. Risk exception
C. Risk treatment
D. Risk response

Answer: D

NEW QUESTION 271
- (Exam Topic 15)
Which of the following BEST describes the purpose of software forensics?

A. To perform cyclic redundancy check (CRC) verification and detect changed applications
B. To review program code to determine the existence of backdoors
C. To analyze possible malicious intent of malware
D. To determine the author and behavior of the code

Answer: D

NEW QUESTION 276
- (Exam Topic 15)
A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

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

Answer: B

NEW QUESTION 279
- (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 280
- (Exam Topic 15)
What is the MOST significant benefit of role-based access control (RBAC)?

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

Answer: A

NEW QUESTION 282
- (Exam Topic 15)
When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

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

Answer: C

NEW QUESTION 284
- (Exam Topic 15)
Which of the following BEST obtains an objective audit of security controls?

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

Answer: A

NEW QUESTION 285
- (Exam Topic 15)
An access control list (ACL) on a router is a feature MOST similar to which type of firewall?

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

Answer: B

NEW QUESTION 288
- (Exam Topic 15)
Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

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

Answer: A

NEW QUESTION 289
- (Exam Topic 15)
An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

A. Engage a third-party auditing firm.
B. Review security architecture.
C. Perform incremental assessments.
D. Conduct penetration testing.

Answer: C

NEW QUESTION 290
- (Exam Topic 15)
Which of the following MUST be done before a digital forensics investigator may acquire digital evidence?

A. Inventory the digital evidence.
B. Isolate the digital evidence.
C. Verify that the investigator has the appropriate legal authority to proceed.
D. Perform hashing to verify the integrity of the digital evidence.

Answer: C

NEW QUESTION 291
- (Exam Topic 15)
A new site's gateway isn't able to form a tunnel to the existing site-to-site Internet Protocol Security (IPsec) virtual private network (VPN) device at headquarters. Devices at the new site have no problem accessing resources on the Internet. When testing connectivity between the remote site’s gateway, it was observed that the external Internet Protocol (IP) address of the gateway was set to 192.168.1.1. and was configured to send outbound traffic to the Internet Service Provider (ISP) gateway at4 192.168.1.2. Which of the following would be the BEST way to resolve the issue and get the remote site connected?

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

Answer: A

NEW QUESTION 292
- (Exam Topic 15)
During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

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

Answer: B

NEW QUESTION 296
- (Exam Topic 15)
A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?

A. Username and personal identification number (PIN)
B. Fingerprint and retinal scanners
C. Short Message Services (SMS) and smartphone authenticator
D. Hardware token and password

Answer: D

NEW QUESTION 300
- (Exam Topic 15)
Which of the following attack types can be used to compromise the integrity of data during transmission?

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

Answer: B

NEW QUESTION 301
- (Exam Topic 15)
A recent security audit is reporting several unsuccessful login attempts being repeated at specific times during the day on an Internet facing authentication server. No alerts have been generated by the security information and event management (SIEM) system. What PRIMARY action should be taken to improve SIEM performance?

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

Answer: B

NEW QUESTION 306
- (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 308
- (Exam Topic 15)
What is the FIRST step in developing a patch management plan?

A. Subscribe to a vulnerability subscription service.
B. Develop a patch testing procedure.
C. Inventory the hardware and software used.
D. Identify unnecessary services installed on systems.

Answer: B

NEW QUESTION 313
- (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 317
- (Exam Topic 15)
A Chief Information Officer (CIO) has delegated responsibility of their system security to the head of the information technology (IT) department. While corporate policy dictates that only the CIO can make decisions on the level of data protection required, technical implementation decisions are done by the head of the IT department. Which of the following BEST describes the security role filled by the head of the IT department?

A. System analyst
B. System security officer
C. System processor
D. System custodian

Answer: D

NEW QUESTION 320
- (Exam Topic 15)
A software development company found odd behavior in some recently developed software, creating a need for a more thorough code review. What is the MOST effective argument for a more thorough code review?

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

Answer: D

NEW QUESTION 321
- (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 326
- (Exam Topic 15)
Digital non-repudiation requires which of the following?

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

Answer: A

NEW QUESTION 329
- (Exam Topic 15)
Which of the following is the MOST important first step in preparing for a security audit?

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

Answer: B

NEW QUESTION 334
- (Exam Topic 15)
Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

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

Answer: C

NEW QUESTION 336
- (Exam Topic 15)
Which of the following encryption technologies has the ability to function as a stream cipher?

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

Answer: A

NEW QUESTION 338
- (Exam Topic 15)
Which technique helps system designers consider potential security concerns of their systems and applications?

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

Answer: B

NEW QUESTION 340
- (Exam Topic 15)
Of the following, which BEST provides non- repudiation with regards to access to a server room?

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

Answer: C

NEW QUESTION 344
- (Exam Topic 15)
An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

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

Answer: A

NEW QUESTION 346
- (Exam Topic 15)
Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

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

Answer: C

NEW QUESTION 350
- (Exam Topic 15)
A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

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

Answer: B

NEW QUESTION 354
- (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 358
- (Exam Topic 15)
An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 1
B. 2
C. 3

Answer: A

NEW QUESTION 363
- (Exam Topic 15)
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

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

Answer: D

NEW QUESTION 365
- (Exam Topic 15)
Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

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

Answer: A

NEW QUESTION 368
- (Exam Topic 15)
A large manufacturing organization arranges to buy an industrial machine system to produce a new line of products. The system includes software provided to the vendor by a thirdparty organization. The financial risk to the manufacturing organization starting production is high. What step should the manufacturing organization take to minimize its financial risk in the new venture prior to the purchase?

A. Hire a performance tester to execute offline tests on a system.
B. Calculate the possible loss in revenue to the organization due to software bugs and vulnerabilities, and compare that to the system's overall price.
C. Place the machine behind a Layer 3 firewall.
D. Require that the software be thoroughly tested by an accredited independent software testing company.

Answer: B

NEW QUESTION 373
- (Exam Topic 15)
What is the BEST method to use for assessing the security impact of acquired software?

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

Answer: B

NEW QUESTION 376
- (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 379
- (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 384
- (Exam Topic 15)
Secure coding can be developed by applying which one of the following?

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

Answer: B

NEW QUESTION 386
- (Exam Topic 15)
International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

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

Answer: C

NEW QUESTION 391
- (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 395
- (Exam Topic 15)
A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

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

Answer: B

NEW QUESTION 399
- (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 402
- (Exam Topic 15)
An employee's home address should be categorized according to which of the following references?

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

Answer: B

NEW QUESTION 403
- (Exam Topic 15)
When developing an organization's information security budget, it is important that the

A. expected risk can be managed appropriately with the funds allocated.
B. requested funds are at an equal amount to the expected cost of breaches.
C. requested funds are part of a shared funding pool with other areas.
D. expected risk to the organization does not exceed the funds allocated.

Answer: A

NEW QUESTION 405
- (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 407
- (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 410
- (Exam Topic 15)
While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

A. Detective and recovery controls
B. Corrective and recovery controls
C. Preventative and corrective controls
D. Recovery and proactive controls

Answer: C

NEW QUESTION 411
- (Exam Topic 15)
Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

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

Answer: C

NEW QUESTION 412
- (Exam Topic 15)
A firm within the defense industry has been directed to comply with contractual requirements for encryption of a government client’s Controlled Unclassified Information (CUI). What encryption strategy represents how to protect data at rest in the MOST efficient and cost-effective manner?

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

Answer: C

NEW QUESTION 415
- (Exam Topic 15)
When conducting a remote access session using Internet Protocol Security (IPSec), which Open Systems Interconnection (OSI) model layer does this connection use?

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

Answer: B

NEW QUESTION 416
- (Exam Topic 15)
Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

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

Answer: A

NEW QUESTION 418
- (Exam Topic 15)
Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

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

Answer: A

NEW QUESTION 419
- (Exam Topic 15)
What is considered a compensating control for not having electrical surge protectors installed?

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

Answer: D

NEW QUESTION 424
- (Exam Topic 15)
Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

A. Training
B. Legal
C. Business
D. Storage

Answer: B

NEW QUESTION 428
- (Exam Topic 15)
A Certified Information Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to4 perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)? Code of Professional Ethics, which of the following should the CISSP do?

A. Review the CISSP guidelines for performing a vulnerability assessment before proceeding to complete it
B. Review the PCI requirements before performing the vulnerability assessment
C. Inform the CISO that they are unable to perform the task because they should render only those services for which they are fully competent and qualified
D. Since they are CISSP certified, they have enough knowledge to assist with the request, but will need assistance in order to complete it in a timely manner

Answer: C

NEW QUESTION 431
- (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 436
- (Exam Topic 15)
Which of the following is the BEST method to gather evidence from a computer's hard drive?

A. Disk duplication
B. Disk replacement
C. Forensic signature
D. Forensic imaging

Answer: D

NEW QUESTION 437
- (Exam Topic 15)
An organization implements Network Access Control (NAC) ay Institute of Electrical and Electronics Engineers (IEEE) 802.1x and discovers the printers do not support the IEEE 802.1x standard. Which of the following is the BEST resolution?

A. Implement port security on the switch ports for the printers.
B. Implement a virtual local area network (VLAN) for the printers.
C. Do nothing; IEEE 802.1x is irrelevant to printers.
D. Install an IEEE 802. 1x bridge for the printers.

Answer: A

NEW QUESTION 442
- (Exam Topic 15)
Which of the following BEST describes the use of network architecture in reducing corporate risks associated with mobile devices?

A. Maintaining a "closed applications model on all mobile devices depends on demilitarized 2one (DM2) servers
B. Split tunneling enabled for mobile devices improves demilitarized zone (DMZ) security posture
C. Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices
D. Applications that manage mobile devices are located in an Internet demilitarized zone (DMZ)

Answer: C

NEW QUESTION 447
- (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 451
- (Exam Topic 15)
Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

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

Answer: C

NEW QUESTION 452
- (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 455
- (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 456
- (Exam Topic 15)
Which of the following VPN configurations should be used to separate Internet and corporate traffic?

A. Split-tunnel
B. Remote desktop gateway
C. Site-to-site
D. Out-of-band management

Answer: A

NEW QUESTION 460
- (Exam Topic 15)
A security professional is assessing the risk in an application and does not take into account any mitigating or compensating controls. This type of risk rating is an example of which of the following?

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

Answer: B

NEW QUESTION 461
- (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 464
- (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 467
- (Exam Topic 15)
A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to on and security However, an attacker was able to spoof a registered account on the network and query the SAML provider.
What is the MOST common attack leverage against this flaw?

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

Answer: A

NEW QUESTION 468
- (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 469
- (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 471
- (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 474
- (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 477
- (Exam Topic 15)
A company-wide penetration test result shows customers could access and read files through a web browser. Which of the following can be used to mitigate this vulnerability?

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

Answer: B

NEW QUESTION 479
- (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 483
- (Exam Topic 15)
Which of the following should be included in a good defense-in-depth strategy provided by object-oriented programming for software deployment?

A. Polyinstantiation
B. Polymorphism
C. Encapsulation
D. Inheritance

Answer: A

NEW QUESTION 486
- (Exam Topic 15)
The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in which role in order to ensure proper protection of data during and after the cloud migration?

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

D. Chief Security Officer (CSO)

Answer: A

NEW QUESTION 489
- (Exam Topic 15)
A hospital's building controls system monitors and operates the environmental equipment to maintain a safe and comfortable environment. Which of the following could be
used to minimize the risk of utility supply interruption?

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

Answer: D

NEW QUESTION 490
- (Exam Topic 15)
Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

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

Answer: C

NEW QUESTION 495
- (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 500
- (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 502
- (Exam Topic 15)
Which of the following is a canon of the (ISC)2 Code of Ethics?

A. Integrity first, association before serf, and excellence in all we do
B. Perform all professional activities and duties in accordance with all applicable laws and the highest ethical standards.
C. Provide diligent and competent service to principals.
D. Cooperate with others in the interchange of knowledge and ideas for mutual security.

Answer: C

NEW QUESTION 506
- (Exam Topic 15)
Which of the following is a risk matrix?

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

Answer: C

NEW QUESTION 510
- (Exam Topic 15)
What is the PRIMARY purpose of auditing, as it relates to the security review cycle?

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

Answer: A

NEW QUESTION 515
- (Exam Topic 15)
What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

A. Implement egress filtering at the organization's network boundary.
B. Implement network access control lists (ACL).
C. Implement a web application firewall (WAF).
D. Implement an intrusion prevention system (IPS).

Answer: B

NEW QUESTION 519
- (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 521
- (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 523
- (Exam Topic 15)
Which of the following techniques evaluates the secure design principles of network OF software architectures?

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

Answer: B

NEW QUESTION 526
- (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 529
- (Exam Topic 15)
What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

A. Randomizing data
B. Swapping data
C. Encrypting data
D. Encoding data

Answer: C

NEW QUESTION 534
- (Exam Topic 15)
What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

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

Answer: C

NEW QUESTION 538
- (Exam Topic 15)
A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

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

Answer: D

NEW QUESTION 542
- (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 547
- (Exam Topic 15)
Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

A. Statement on Auditing Standards (SAS) 70
B. Service Organization Control (SOC) 2
C. Service Organization Control (SOC) 1
D. Statement on Standards for Attestation Engagements (SSAE) 18

Answer: B

NEW QUESTION 552
- (Exam Topic 15)
A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several ‘open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

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

Answer: C

NEW QUESTION 554
- (Exam Topic 15)
Which of the fallowing statements is MOST accurate regarding information assets?

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

Answer: B

NEW QUESTION 556
- (Exam Topic 15)

What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

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

Answer: D

NEW QUESTION 559
- (Exam Topic 15)
What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

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

Answer: D

NEW QUESTION 563
- (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 565
- (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 569
- (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 573
- (Exam Topic 14)
Which of the following media is LEAST problematic with data remanence?

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

Answer: A

NEW QUESTION 576
- (Exam Topic 14)
What should an auditor do when conducting a periodic audit on media retention?

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

Answer: A

NEW QUESTION 578

- (Exam Topic 14)
Which of the following is TRUE regarding equivalence class testing?

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

Answer: C

NEW QUESTION 579
- (Exam Topic 14)
An organization wants to enable uses to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (F1M). Which of the following is used behind the scenes in a FIM deployment?

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

Answer: C

NEW QUESTION 583
- (Exam Topic 14)
An organization is considering outsourcing applications and data to a Cloud Service Provider (CSP). Which of the following is the MOST important concern regarding privacy?

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

Answer: D

NEW QUESTION 588
- (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 591
- (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 594
- (Exam Topic 14)
Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities?

A. Definitions for each exposure type
B. Vulnerability attack vectors
C. Asset values for networks
D. Exploit code metrics

Answer: C

NEW QUESTION 596
- (Exam Topic 14)
Which of the following encryption types is used in Hash Message Authentication Code (HMAC) for key distribution?

A. Symmetric
B. Asymmetric

C. Ephemeral
D. Permanent

Answer: A

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

NEW QUESTION 601
- (Exam Topic 14)
Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?

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

Answer: D

NEW QUESTION 603
- (Exam Topic 14)
Additional padding may be added to toe Encapsulating Security Protocol (ESP) b trailer to provide which of the following?

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

Answer: C

NEW QUESTION 604
- (Exam Topic 14)
Which of the following is mobile device remote fingerprinting?

A. Installing an application to retrieve common characteristics of the device
B. Storing information about a remote device in a cookie file
C. Identifying a device based on common characteristics shared by all devices of a certain type
D. Retrieving the serial number of the mobile device

Answer: C

NEW QUESTION 606
- (Exam Topic 14)
Which is the MOST critical aspect of computer-generated evidence?

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

Answer: B

NEW QUESTION 610
- (Exam Topic 14)
Which of the following four iterative steps are conducted on third-party vendors in an on-going basis?

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

Answer: C

NEW QUESTION 611
- (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 614
- (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 616
- (Exam Topic 14)
Which of the following is used to detect steganography?

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

Answer: C

NEW QUESTION 618
- (Exam Topic 14)
A user downloads a file from the Internet, then applies the Secure Hash Algorithm 3 (SHA-3c?

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

Answer: A

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

NEW QUESTION 619
- (Exam Topic 14)
When dealing with shared, privilaged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

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

Answer: B

NEW QUESTION 620
- (Exam Topic 14)
Which is the RECOMMENDED configuration mode for sensors for an intrusion prevention system (IPS) if the prevention capabilities will be used?

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

Answer: C

NEW QUESTION 624
- (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 625
- (Exam Topic 14)
An organization operates a legacy Industrial Control System (ICS) to support its core business service, which carrot be replaced. Its management MUST be performed remotely through an administrative console software, which in tum depends on an old version of the Java Runtime Environment (JPE) known to be vulnerable to a number of attacks, How is this risk BEST managed?

A. Isolate the full ICS by moving It onto its own network segment

B. Air-gap and harden the host used for management purposes
C. Convince the management to decommission the ICS and mitigate to a modem technology
D. Deploy a restrictive proxy between all clients and the vulnerable management station

Answer: B

NEW QUESTION 626
- (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 631
- (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 636
- (Exam Topic 14)
An organization that has achieved a Capability Maturity model Integration (CMMI) level of 4 has done which of the following?

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

Answer: C

NEW QUESTION 640
- (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 643
- (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 645
- (Exam Topic 14)
Which of the following MUST a security professional do in order to quantify the value of a security program to organization management?

A. Report using metrics.
B. Rank priorities as high, medium, or low.
C. Communicate compliance obstacles.
D. Report en employee activities

Answer: A

NEW QUESTION 648
- (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 649
- (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 650
- (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 651
- (Exam Topic 14)
Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?

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

Answer: B

NEW QUESTION 653
- (Exam Topic 14)
Which of the following BEST provides for non-repudiation od user account actions?

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

Answer: D

NEW QUESTION 655
- (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 659
- (Exam Topic 14)
Point-to-Point Protocol (PPP) was designed to specifically address what issue?

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

Answer:

B

NEW QUESTION 660
- (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 661
- (Exam Topic 14)
A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

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

Answer: B

NEW QUESTION 665
- (Exam Topic 14)
Which of the following is the BEST statement for a professional to include as port of business continuity (BC) procedure?

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

Answer: D

NEW QUESTION 668
- (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 671
- (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 674
- (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 677

- (Exam Topic 14)
Which of the following is the PRIMARY reason a sniffer operating on a network is collecting packets only from its own host?

A. An Intrusion Detection System (IDS) has dropped the packets.
B. The network is connected using switches.
C. The network is connected using hubs.
D. The network's firewall does not allow sniffing.

Answer: A

NEW QUESTION 680
- (Exam Topic 14)
How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

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

Answer: A

NEW QUESTION 682
- (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 686
- (Exam Topic 14)
If virus infection is suspected, which of the following is the FIRST step for the user to take?

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

Answer: C

NEW QUESTION 691
- (Exam Topic 14)
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

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

Answer: C

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

NEW QUESTION 693
- (Exam Topic 14)
A vehicle of a private courier company that transports backup data for offsite storage was robbed while in transport backup data for offsite was robbed while in transit. The incident management team is now responsible to estimate the robbery, which of the following would help the incident management team to MOST effectively analyze the business impact of the robbery?

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

Answer: B

NEW QUESTION 698
- (Exam Topic 14)
A new Chief Information Officer (CIO) created a group to write a data retention policy based on applicable laws. Which of the following is the PRIMARY motivation for the policy?

A. To back up data that is used on a daily basis

B. To dispose of data in order to limit liability
C. To reduce costs by reducing the amount of retained data
D. To classify data according to what it contains

Answer: B

NEW QUESTION 699
- (Exam Topic 14)
According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

A. Level 0: Incomplete
B. Level 1: Performed
C. Level 2: Managed
D. Level 3: Defined

Answer: D

NEW QUESTION 704
- (Exam Topic 14)
In fault-tolerant systems, what do rollback capabilities permit?

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

Answer: A

NEW QUESTION 708
- (Exam Topic 14)
Which of the following is the MOST important reason for timely installation of software patches?

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

Answer: C

NEW QUESTION 710
- (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 712
- (Exam Topic 14)
Which of the following is an accurate statement when an assessment results in the discovery of vulnerabilities in a critical network component?

A. The fact that every other host is sufficiently hardened does not change the fact frat the network is placed at risk of attack.
B. There is little likelihood that the entire network is being placed at a significant risk of attack.
C. A second assessment should immediately be performed after all vulnerabilities are corrected.
D. There is a low possibility that any adjacently connected components have been compromised by an attacker

Answer: C

NEW QUESTION 713
- (Exam Topic 14)
Utilizing a public wireless Local Area network (WLAN) to connect to a private network should be done only
in which of the following situations?

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

Answer: A

NEW QUESTION 714

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

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

Answer: B

NEW QUESTION 717
- (Exam Topic 14)
Which of the following can be used to calculate the loss event probability?

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

Answer: B

NEW QUESTION 719
- (Exam Topic 14)
Which of the following practices provides the development of security and identification of threats in designing software?

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

Answer: D

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

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

Answer: C

NEW QUESTION 726
- (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 728
- (Exam Topic 14)
Digital certificates used transport Layer security (TLS) support which of the following?

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

Answer: A

NEW QUESTION 731
- (Exam Topic 14)
When a system changes significantly, who is PRIMARILY responsible for assessing the security impact?

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

Answer: B

NEW QUESTION 734
- (Exam Topic 14)
Which of the following is a characteristic of a challenge/response authentication process?

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

Answer: A

NEW QUESTION 737
- (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 739
- (Exam Topic 14)
What is the MAIN reason to ensure the appropriate retention periods are enforced for data stored on electronic media?

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

Answer: D

NEW QUESTION 740
- (Exam Topic 14)
Which of the following initiates the system recovery phase of a disaster recovery plan?

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

Answer: C

NEW QUESTION 742
- (Exam Topic 14)
Who is essential for developing effective test scenarios for disaster recovery (DR) test plans?

A. Business line management and IT staff members
B. Chief Information Officer (CIO) and DR manager
C. DR manager end IT staff members
D. IT staff members and project managers

Answer: B

NEW QUESTION 744
- (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 745
- (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 750
- (Exam Topic 14)
Directive controls are a form of change management policy and procedures. Which of the following subsections are recommended as part of the change management process?

A. Build and test
B. Implement security controls
C. Categorize Information System (IS)
D. Select security controls

Answer: A

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

NEW QUESTION 751
- (Exam Topic 14)
Information security metrics provide the GREATEST value tp management when based upon the security manager's knowledge of which of the following?

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

Answer: B

NEW QUESTION 752
- (Exam Topic 14)
Which of the following is the PRIMARY security consideration for how an organization should handle Information Technology (IT) assets?

A. The monetary value of the asset
B. The controls implemented on the asset
C. The physical form factor of the asset
D. The classification of the data on the asset

Answer: D

NEW QUESTION 753
- (Exam Topic 14)
Which of the following MUST be considered when developing business rules for a data loss prevention (DLP) solution?

A. Data availability
B. Data sensitivity
C. Data ownership
D. Data integrity

Answer: B

NEW QUESTION 756
- (Exam Topic 14)
Which of the following methods MOST efficiently manages user accounts when using a third-party cloud-based application and directory solution?

A. Cloud directory
B. Directory synchronization
C. Assurance framework
D. Lightweight Directory Access Protocol (LDAP)

Answer: B

NEW QUESTION 759
- (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 763
- (Exam Topic 14)
Which one of the following would cause an immediate review and possible change to the security policies of an organization?

A. Change in technology
B. Change in senior management
C. Change to organization processes
D. Change to organization goals

Answer: D

NEW QUESTION 768
- (Exam Topic 14)
Which of the following is applicable to a publicly held company concerned about information handling and storage requirement specific to the financial reporting?

A. Privacy Act of 1974
B. Clinger-Cohan Act of 1996
C. Sarbanes-Oxley (SOX) Act of 2002
D. International Organization for Standardization (ISO) 27001

Answer: C

NEW QUESTION 770
- (Exam Topic 14)
Why is planning the MOST critical phase of a Role Based Access Control (RBAC) implementation?

A. The criteria for measuring risk is defined.
B. User populations to be assigned to each role is determined.
C. Role mining to define common access patterns is performed.
D. The foundational criteria are defined.

Answer: B

NEW QUESTION 771
- (Exam Topic 14)
Which of the following is MOST important when determining appropriate countermeasures for an identified risk?

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

Answer: C

NEW QUESTION 774
- (Exam Topic 14)
Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

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

Answer: A

NEW QUESTION 777
- (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 781
- (Exam Topic 14)
Individual access to a network is BEST determined based on

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

Answer:

C

NEW QUESTION 786
- (Exam Topic 14)
What is maintained by using write blocking devices whan forensic evidence is examined?

A. Inventory
B. Integrity
C. Confidentiality
D. Availability

Answer: B

NEW QUESTION 790
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

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

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