ISC.CISSP.v2020-11-01.q312

Exam Code:	CISSP
Exam Name:	Certified Information Systems Security Professional (CISSP)
Certification Provider:	ISC
Free Question Number:	312
Version:	v2020-11-01
# of views:	3939
# of Questions views:	225267
https://www.freecram.net/torrent/ISC.CISSP.v2020-11-01.q312.html	

NEW QUESTION: 1
The birthday attack is MOST effective against which one of the following cipher technologies?
A. Chaining block encryption
B. Cryptographic hash
C. Asymmetric cryptography
D. Streaming cryptography
Answer: (SHOW ANSWER)

NEW QUESTION: 2
When implementing a data classification program, why is it important to avoid too much granularity?
A. It will be difficult to assign ownership to the data
B. It will be difficult to apply to both hardware and software
C. The process will require too many resources
D. The process will be perceived as having value
Answer: (SHOW ANSWER)

NEW QUESTION: 3
The BEST way to check for good security programming practices, as well as auditing for possible backdoors, is to conduct
A. impact assessments.
B. static analysis.
C. log auditing.
D. code reviews.
Answer: (SHOW ANSWER)

NEW QUESTION: 4

A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?
A. The organization's current security policies concerning privacy issues
B. Privacy-related regulations enforced by governing bodies applicable to the organization
C. Privacy best practices published by recognized security standards organizations
D. Organizational procedures designed to protect privacy information
Answer: (SHOW ANSWER)

NEW QUESTION: 5
The core component of Role Based Access control (RBAC) must be constructed of defined data elements, Which elements are requried?
A. Users, rotes, operations, and protected objects
B. Roles, accounts, permissions, and protected objects
C. Users, permissions, operators, and protected objects
D. Roles, operations, accounts, and protected objects
Answer: (SHOW ANSWER)

NEW QUESTION: 6
A vulnerability in which of the following components would be MOST difficult to detect?
A. Shared libraries
B. Kernel
C. Hardware
D. System application
Answer: (SHOW ANSWER)

NEW QUESTION: 7
An engineer in a software company has created a virus creation tool. The tool can generate thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled environment to test the company's next generation virus scanning software. Which would BEST describe the behavior of the engineer and why?
A. The behavior is not ethical because creating any kind of virus is bad.
B. The behavior is ethical because the tool will be used to create a better virus scanner.
C. The behavior is not ethical because such a tool could be leaked on the Internet.
D. The behavior is ethical because any experienced programmer could create such a tool.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?
A. In-house Network Team
B. Disaster Recovery (DR) Team

C. In-house security administrators
D. External consultants
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?
A. To assure the software development team that all security issues have been addressed
B. To verify that security protection remains acceptable to the organizational security policy
C. To assist data owners in making future sensitivity and criticality determinations
D. To help the security team accept or reject new systems for implementation and production
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?

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

NEW QUESTION: 11
When implementing controls in a heterogeneous end-point network for an organization, it is critical that
A. common software security components be implemented across all hosts.
B. hosts are able to establish network communications.
C. users can make modifications to their security software configurations.
D. firewalls running on each host are fully customizable by the user.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Change management policies and procedures belong to which of the following types of controls?
A. Directive
B. Detective
C. Corrective
D. Preventative
Answer: (SHOW ANSWER)
Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC pg=PA570&lpg=PA570&dq=CISSP+Change+management+policies+and+procedures+belong+to+which+type+of+control&

source=bl&ots=riGvVpUO4H&sig=ACfU3U0kRWWaIlj7gwqlovVku880wG5LOg&hl=en&sa=X&ved=2ahUKEwjA7cGL_anpAhULxoUKHc1lD3UQ6AEwCnoECBIQAQ#v=onepage& q=CISSP%20Change%20management%20policies%20and%20procedures%20belong%20to%20which%&f=false

NEW QUESTION: 13
Which of the following is a method of attacking internet protocol (IP) v6 Layer 3 and Layer 4?
A. Synchronize sequence numbers (SYN) flooding
B. Internet Control Message Protocol (ICMP) flooding
C. Media Access Control (MAC) flooding
D. Domain Name Server (DNS) cache poisoning
Answer: (SHOW ANSWER)

NEW QUESTION: 14
A company receives an email threat informing of an Imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques BEST addresses that threat?
A. Set Up Web Application Firewalls (WAFs) to filter out malicious traffic
B. Deploying load balancers to distribute inbound traffic across multiple data centers
C. Coordinate with and utilize capabilities within Internet Service Provider (ISP)
D. Implementing reverse web-proxies to validate each new inbound connection
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which of the following would present the highert annualized loss expectancy (ALE)?

Event	Loss Expectancy	Annualized Rate of Occurrence	Insurance Coverage
Fire	$1,000,000	0.1	80%
Flood	$250,000	0.2	50%
Windstorm	$50,000	0.5	80%
Earthquake	$800,000	0.02	None

A. Windstorm
B. Fire
C. Flood
D. Earthquake
Answer: (SHOW ANSWER)

NEW QUESTION: 16
An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?
A. Employee directory and organizational chart.

B. Limits and scope of the testing.
C. Physical location of server room and wiring closet.
D. Logical location of filters and concentrators.
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following is the PRIMARY security consideration for how an organization should handle Information Technology (IT) assets?
A. The controls implemented on the asset
B. The physical form factor of the asset
C. The classification of the data on the asset
D. The monetary value of the asset
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which of the following explains why record destruction requirements are included in a data retention policy?
A. To meet destruction guidelines
B. To comply with legal and business requirements
C. To validate data ownership
D. To save cost for storage and backup
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?
A. Standardized configurations for devices
B. Standardized patch testing equipment
C. Automated system patching
D. Management support for patching
Answer: (SHOW ANSWER)
Explanation

Section: Security Assessment and Testing

NEW QUESTION: 20

Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

A. An explanation of all the technologies employed by the collecting organization in gathering information on the data subject.

B. An explanation of who can be contacted at the organization collecting the information if corrections are required by the data subject.

C. An explanation of the regulatory frameworks and compliance standards the information collecting organization adheres to.

D. An explanation of how long the data subject's collected information will be retained for and how it will be eventually disposed.

Answer: (SHOW ANSWER)

NEW QUESTION: 21

Which of the following can be used to calculate the loss event probability?

A. Total number of possible outcomes multiplied by frequency of outcomes

B. Total number of possible outcomes divided by frequency of outcomes

C. Number of outcomes divided by total number of possible outcomes

D. Number of outcomes multiplied by total number of possible outcomes

Answer: (SHOW ANSWER)

NEW QUESTION: 22

While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

A. Retention

B. Recovery

C. Remediation

D. Reporting

Answer: (SHOW ANSWER)

NEW QUESTION: 23

Which one of the following is a fundamental objective in handling an incident?

A. To restore control of the affected systems

B. To prosecute the attacker

C. To perform full backups of the system

D. To confiscate the suspect's computers

Answer: (SHOW ANSWER)

NEW QUESTION: 24

Who in the organization is accountable for classification of data information assets?

A. Chief Information Security Officer (CISO)
B. Data architect
C. Chief Information Officer (CIO)
D. Data owner
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following BEST describes Recovery Time Objective (RTO)?
A. Time of data validation after disaster
B. Time of application resumption after disaster
C. Time of data restoration from backup after disaster
D. Time of application verification after disaster
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information form malicious software?
A. Review the code to identify its origin.
B. Examine the file properties and permissions.
C. Analyze the logs generated by the software.
D. Analyze the behavior of the program.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which of the following is the PRIMARY issue when collecting detailed log information?
A. Most systems and applications do not support logging
B. Logs do not provide sufficient details of system and individual activities
C. Logs may be unavailable when required
D. Timely review of the data is potentially difficult
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28
Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?
A. Mobile site
B. Warm site
C. Cold site
D. Hot site
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which of the following PRIMARILY contributes to security incidents in web-based applications?

A. Improper stress testing and application interfaces
B. System incompatibility and patch management
C. Third-party applications and change controls
D. Systems administration and operating systems
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which of the following is the GREATEST security risk associated with the use of identity as a service (IDaaS) when an organization is developing its own software?

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

NEW QUESTION: 31
During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?
A. Create a list to include in the Security Assessment and Authorization package.
B. Calculate the value of assets being accredited.
C. Identify obsolete hardware and software.
D. Define the boundaries of the information system.
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following is the MOST important element of change management documentation?
A. Number of changes being made
B. A stakeholder communication
C. Business case justification
D. List of components involved
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?
A. Use of Network Access Control (NAC) on switches.
B. Use of a unified messaging.
C. Use of separation for the voice network.
D. Use of Request for Comments (RFC) 1918 addressing.
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?
A. variances against regulatory requirements
B. poor governance over security processes and procedures
C. unanticipated increases in security incidents and threats
D. immature security controls and procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 35
All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that
A. Identify the financial impacts of a business interruption
B. Identify the operational impacts of a business interruption
C. determine the risk of a business interruption occurring
D. determine the technological dependence of the business processes
Answer: (SHOW ANSWER)

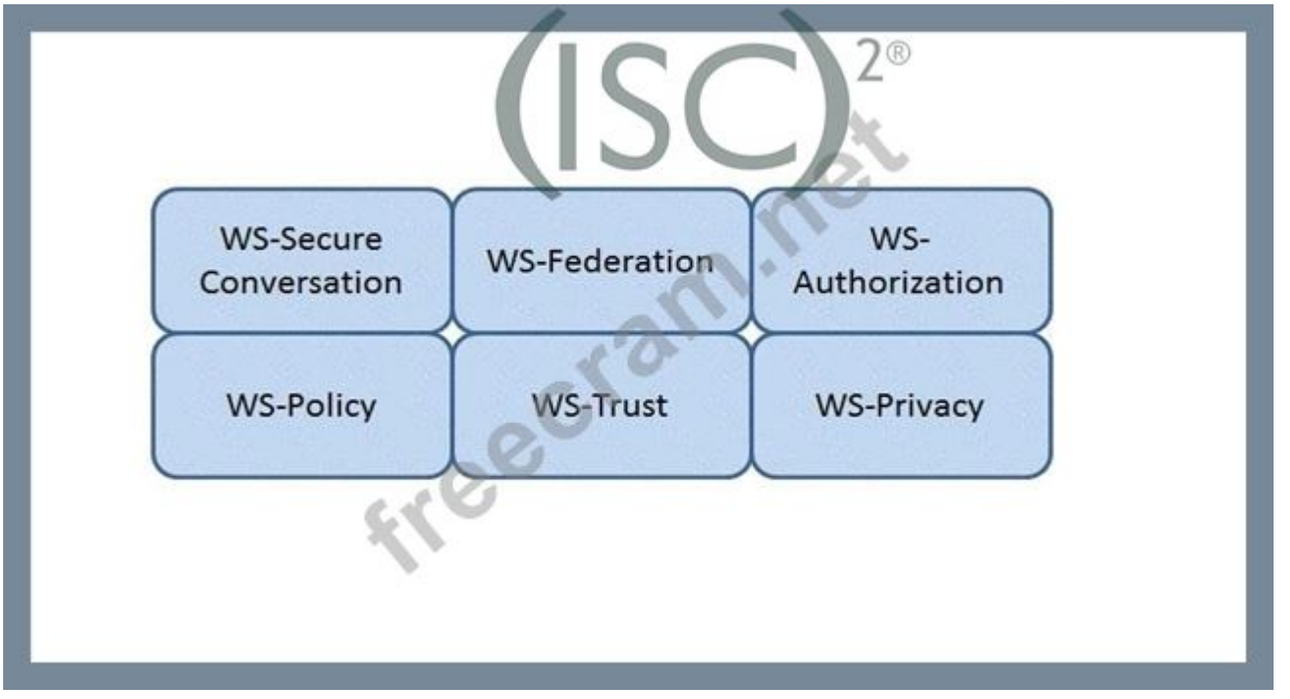
NEW QUESTION: 36
What is the FIRST step required in establishing a records retention program?
A. Identify and inventory all records.
B. Identify and inventory all records storage locations.
C. Classify records based on sensitivity.
D. Draft a records retention policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
What should be the INITIAL response to Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts?
A. Ensure that the Incident Response Plan is available and current.
B. Determine the traffic's initial source and block the appropriate port.
C. Disable or disconnect suspected target and source systems.

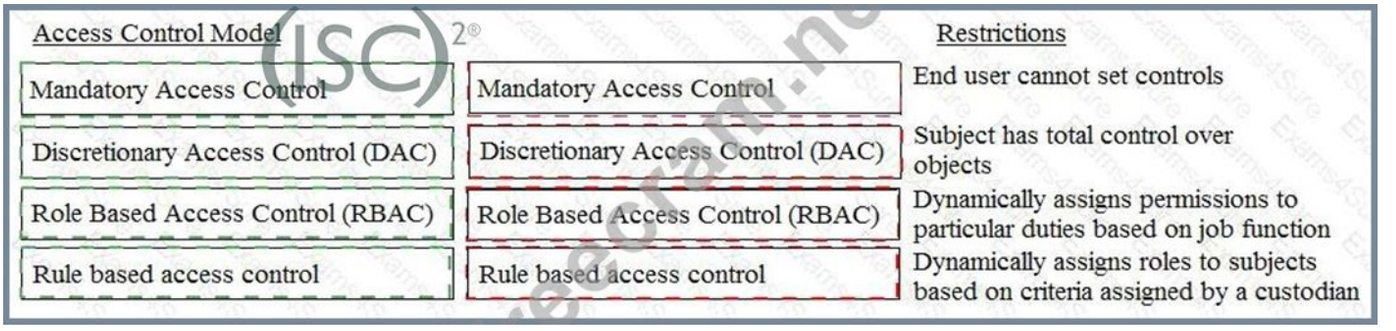
D. Verify the threat and determine the scope of the attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Which of the following is a common feature of an Identity as a Service (IDaaS) solution?
A. Privileged user authentication support
B. Password reset service support
C. Single Sign-On (SSO) authentication support
D. Terminal Access Controller Access Control System (TACACS) authentication support
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



Answer:



Explanation
WS-Trust
The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and

validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.
Reference: https://msdn.microsoft.com/en-us/library/ff650503.aspx

NEW QUESTION: 40

In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

A. Escalation
B. Planning
C. Recovery
D. Communication
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which of the following methods provides the MOST protection for user credentials?
A. Self-registration
B. Forms-based authentication
C. Basic authentication
D. Digest authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?
A. ifconfig
B. dig
C. nbstat
D. ipconfig
Answer: (SHOW ANSWER)

NEW QUESTION: 43
If a content management system (CMC) is implemented, which one of the following would occur?
A. Patching the systems would be completed more quickly
B. The test and production systems would be running the same software
C. The applications placed into production would be secure
D. Developers would no longer have access to production systems
Answer: (SHOW ANSWER)

NEW QUESTION: 44

An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

A. Prevention, detection, and remediation

B. Certification, accreditation, and monitoring

C. Development, testing, and deployment

D. People, technology, and operations

Answer: (SHOW ANSWER)

NEW QUESTION: 45

A security practitioner has been tasked with establishing organizational asset handling procedures.

What should be considered that would have the GRFATEST impact to the development of these procedures?

A. Acceptable Use Policy (ALP)

B. Information classification scheme

C. User roles and responsibilities

D. Media handling procedures

Answer: (SHOW ANSWER)

NEW QUESTION: 46

What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

A. Determining the Recovery Time Objective (RTO)

B. Evaluating the efficiency of the plan

C. Identifying the benchmark required for restoration

D. Validating the effectiveness of the plan

Answer: (SHOW ANSWER)

NEW QUESTION: 47

Which of the following can BEST prevent security flaws occurring in outsourced software development?

A. Contractual requirements for code quality

B. Licensing, code ownership and intellectual property rights

C. Delivery dates, change management control and budgetary control
D. Certification of the quality and accuracy of the work done
Answer: (SHOW ANSWER)

NEW QUESTION: 48
A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected?
A. Trojan horse
B. Man-in-the-Middle (MITM)
C. Denial of Service (DoS)
D. Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 49
The type of authorized interactions a subject can have with an object is
A. protocol.
B. permission.
C. procedure.
D. control.
Answer: (SHOW ANSWER)

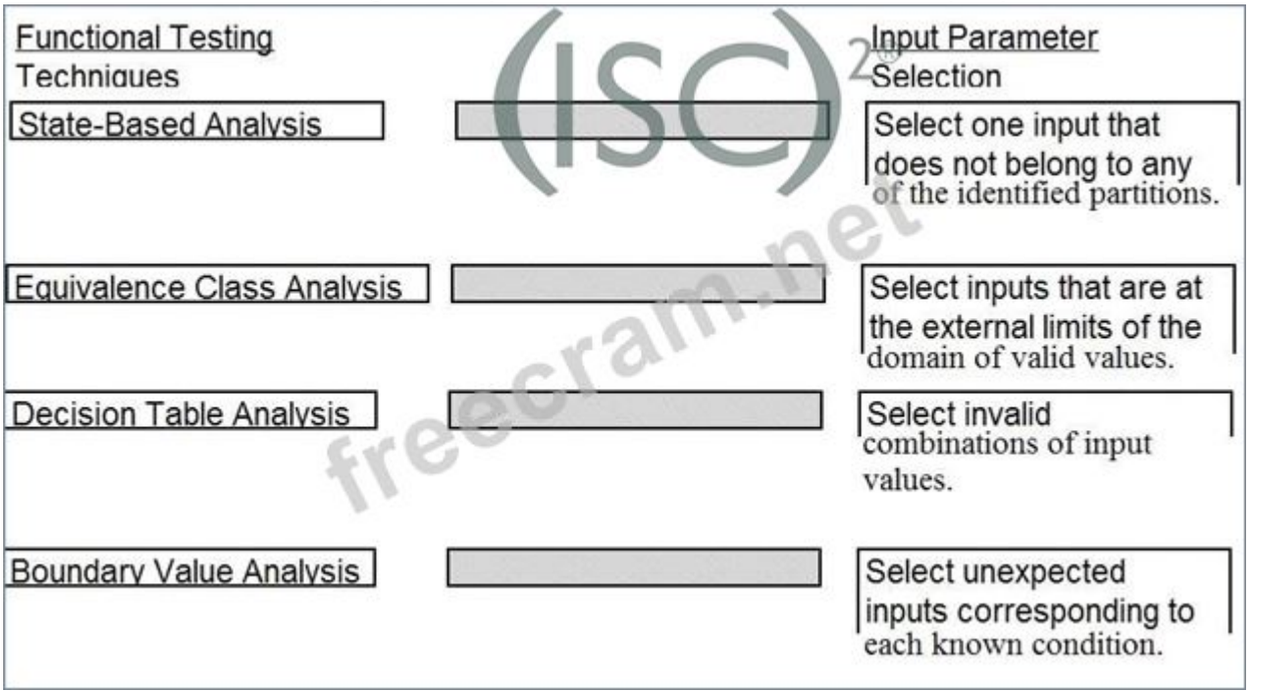
NEW QUESTION: 50
What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

A. Spoofing
B. Man-in-the-Middle (MITM) attack
C. Session redirect
D. Smurfing
Answer: (SHOW ANSWER)

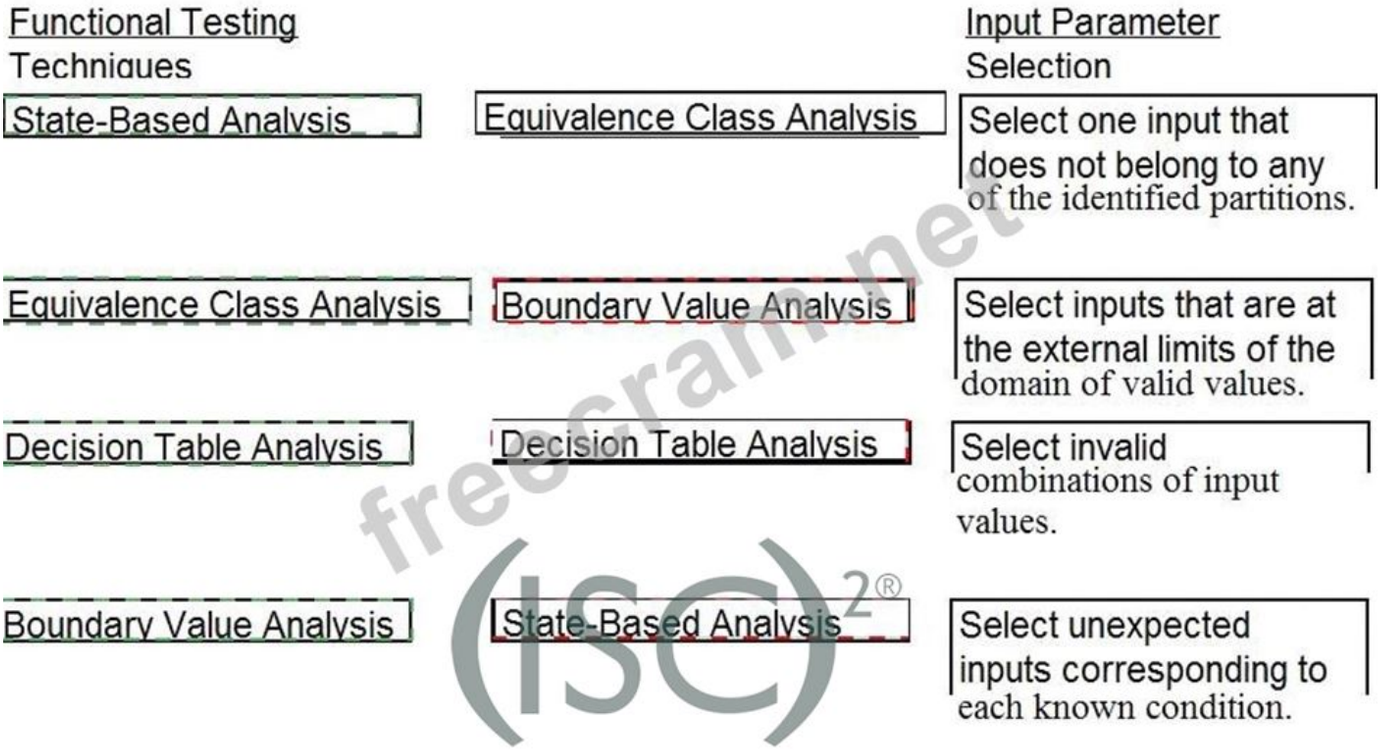
NEW QUESTION: 51
In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?
A. Developers checking out source code without approval
B. Developers using Rapid Application Development (RAD) methodologies without approval
C. Promoting programs to production without approval
D. Modifying source code without approval
Answer: (SHOW ANSWER)

NEW QUESTION: 52

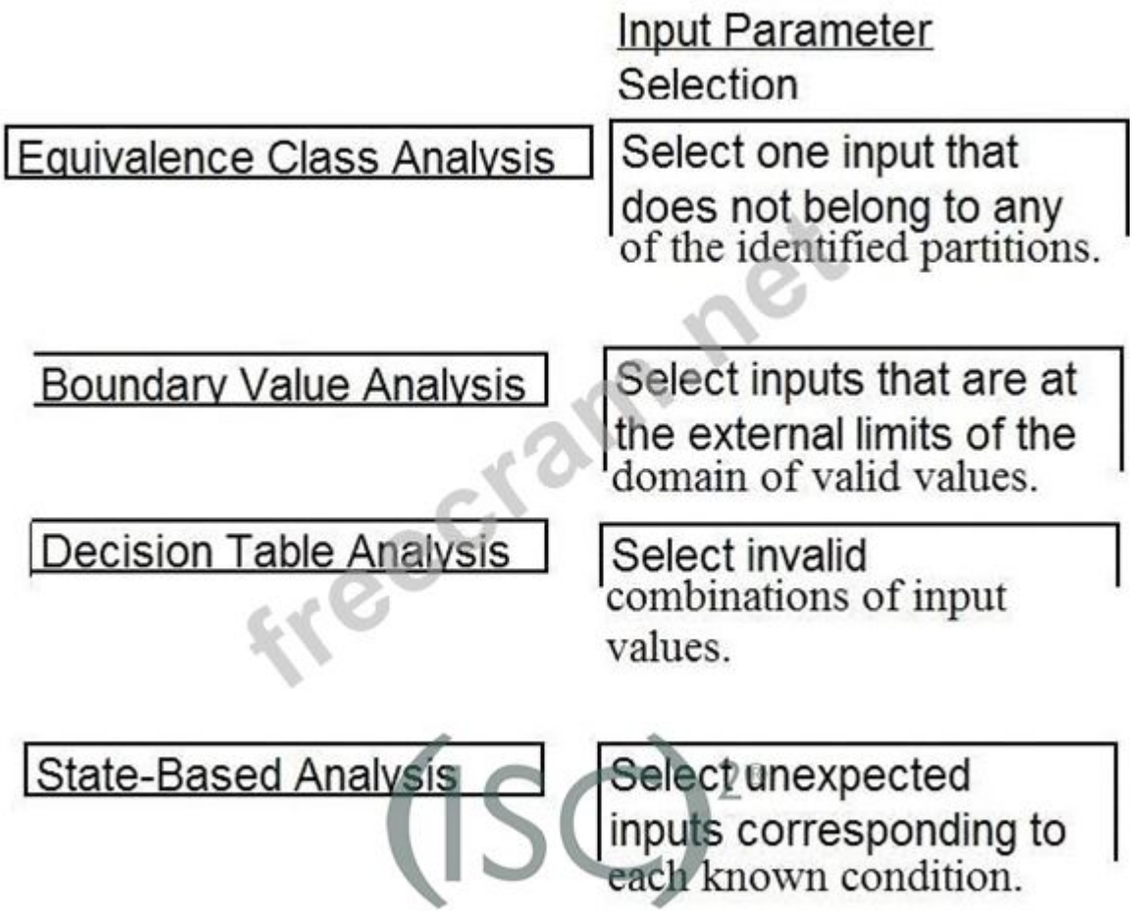
A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.



Answer:



Explanation



NEW QUESTION: 53
Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?
A. Preboot eXecution Environment (PXE)
B. Trusted Platform Module (TPM)
C. Key Distribution Center (KDC)
D. Simple Key-Management for Internet Protocol (SKIP)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 54
Which of the following is the MOST difficult to enforce when using cloud computing?
A. Data backup
B. Data access
C. Data recovery
D. Data disposal
Answer: (SHOW ANSWER)

NEW QUESTION: 55
When transmitting information over public networks, the decision to encrypt it should be based on
A. the volume of the information.

B. the level of confidentiality of the information.
C. the estimated monetary value of the information.
D. whether there are transient nodes relaying the transmission.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?
A. Data access control policies
B. Common Criteria (CC)
C. Business Impact Analysis (BIA)
D. Threat modeling
Answer: (SHOW ANSWER)

NEW QUESTION: 57
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?
A. Require students to purchase home router capable of VPN.
B. Use Secure Shell (SSH) with public/private keys.
C. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.
D. Use Secure Sockets Layer (SSL) VPN technology.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 58
What is a warn site when conducting Business continuity planning (BCP)
A. A location, other than the normal facility, used to process data on a daily basis
B. A place void of any resources or equipment except air conditioning and raised flooring
C. An alternate facility that allows for Immediate cutover to enable continuation of business functions
D. An area partially equipped with equipment and resources to recover business functions
Answer: (SHOW ANSWER)

NEW QUESTION: 59
A user downloads a file from the Internet, then applies the Secure Hash Algorithm 3 (SHA-3) to it. Which of the following is the MOST likely reason for doing so?
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: (SHOW ANSWER)

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

NEW QUESTION: 60

Software Code signing is used as a method of verifying what security concept?

A. Availability

B. Integrity

C. Confidentiality

D. Access Control

Answer: (SHOW ANSWER)

NEW QUESTION: 61

Which of the following is needed to securely distribute symmetric cryptographic keys?

A. Hardware tokens that protect the user's private key.

B. An organizationally approved communication protection policy and key management plan

C. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates

D. Officially approved and compliant key management technology and processes

Answer: (SHOW ANSWER)

NEW QUESTION: 62

A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

A. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

B. Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)

C. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)

D. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Answer: (SHOW ANSWER)

NEW QUESTION: 63

Which of the following MUST an organization do to effectively communicate is security strategy to all affected parties?

A. Remove potential communication barriers.

B. Involve representatives from each key organizational area.

C. Provide regular updates to the board of directors.
D. Notify staff of changes to the strategy.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which of the following initiates the system recovery phase of a disaster recovery plan?
A. Activating the organization
B. Assessing the extent of damage following the disaster
C. Evacuating the disaster site
D. Issuing a formal disaster declaration
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following is a reason to use manual patch installation instead of automated patch management?
A. The cost required to install patches will be reduced.
B. The ability to cover large geographic areas is increased.
C. The likelihood of system or application incompatibilities will be decreased.
D. The time during which systems will remain vulnerable to an exploit will be decreased.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
Which of the following is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services?
A. The risk executive (function)
B. The IT manager
C. The acquiring organization
D. The service provider
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which of the following is critical for establishing an initial baseline for software components in the operation and maintenance of applications?
A. Software patching procedures
B. Configuration control procedures
C. Application monitoring procedures
D. Security audit procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 68

Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

A. The overall protection of corporate resources and data

B. Secondary use of the data by business users

C. The business purpose for which the data is to be used

D. The organization's security policies and standards

Answer: (SHOW ANSWER)

NEW QUESTION: 69

Why must all users be positively identified prior to using multi-user computers?

A. To provide access to system privileges

B. To ensure that unauthorized persons cannot access the computers

C. To ensure that management knows what users are currently logged on

D. To provide access to the operating system

Answer: (SHOW ANSWER)

NEW QUESTION: 70

Which of the following is the BEST reason for writing an information security policy?

A. To support information security governance

B. To deter attackers

C. To reduce the number of audit findings

D. To implement effective information security controls

Answer: (SHOW ANSWER)

NEW QUESTION: 71

Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

A. Validate target systems have been backed up.

B. Ensure firewall logging has been activated.

C. Verify countermeasures have been deactivated.

D. Confirm warm site is ready to accept connections.

Answer: (SHOW ANSWER)

NEW QUESTION: 72

Which of the following MOST influences the design of the organization's electronic monitoring policies?

A. Level of organizational trust

B. Business ethical considerations

C. Results of background checks

D. Workplace privacy laws

Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?
A. WEP uses Message Digest 5 (MD5)
B. WEP uses a small range Initialization Vector (IV)
C. WEP uses Diffie-Hellman
D. WEP does not use any Initialization Vector (IV)
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following is the BEST reason for the use of security metrics?
A. They ensure that the organization meets its security objectives.
B. They speed up the process of quantitative risk assessment.
C. They provide an appropriate framework for Information Technology (IT) governance.
D. They quantify the effectiveness of security processes.
Answer: (SHOW ANSWER)

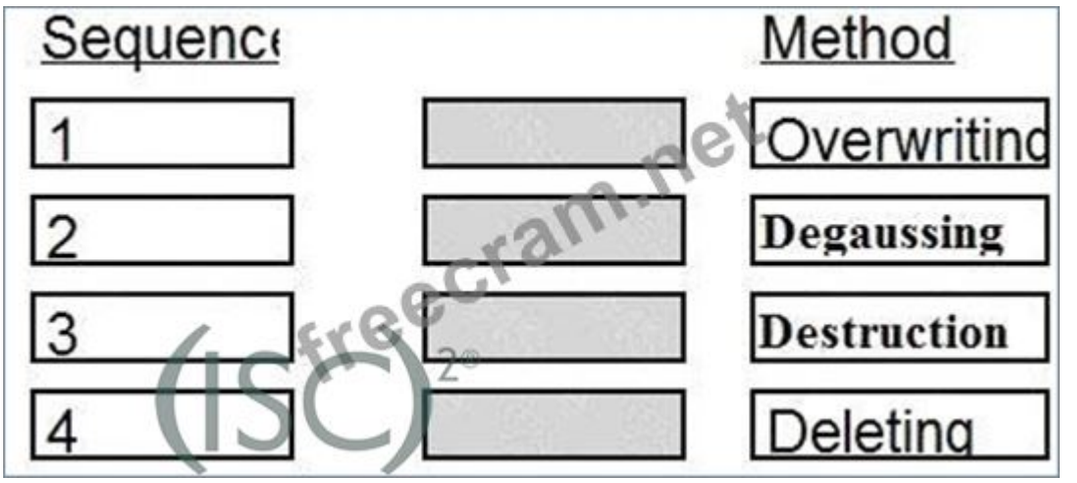
NEW QUESTION: 75
Which of the following was developed to support multiple protocols as well as provide as well as provide login, password, and error correction capabilities?
A. Post Office Protocol (POP)
B. Password Authentication Protocol (PAP)
C. Point-to-Point Protocol (PPP)
D. Challenge Handshake Authentication Protocol (CHAP)
Answer: (SHOW ANSWER)

NEW QUESTION: 76
An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.
Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?
A. The audit reports have been issued in the last six months.
B. The audit assessment has been conducted by an international audit firm.
C. The audit assessment has been conducted by an independent assessor.
D. The audit reports have been signed by the third-party senior management.
Answer: (SHOW ANSWER)

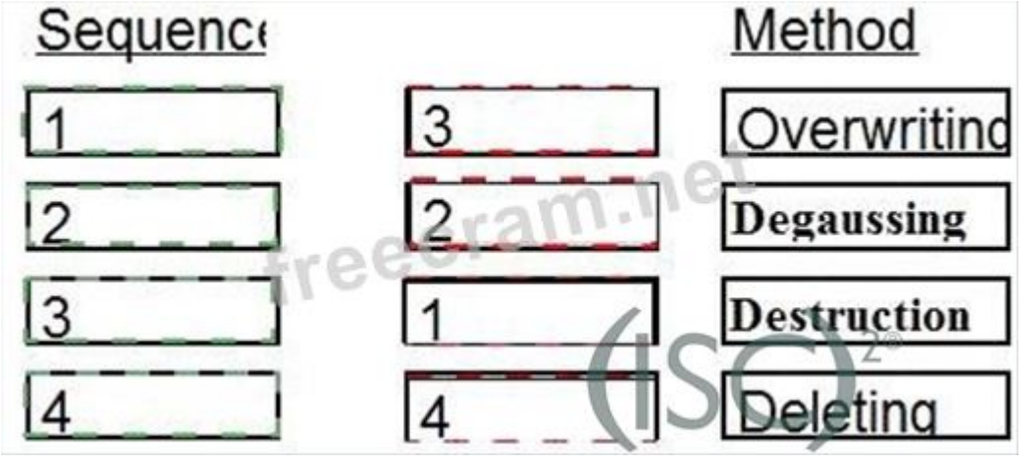
NEW QUESTION: 77
A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?
A. Obfuscated code
B. Random number generator
C. Encryption routines
D. Botnet command and control
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?
A. Integrity
B. Confidentiality
C. Accountability
D. Availability
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic mediA.



Answer:



Explanation

NEW QUESTION: 80

Which of the following is a responsibility of a data steward?

A. Document data governance requirements.

B. Ensure that data decisions and impacts are communicated to the organization.

C. Conduct data governance interviews with the organization.

D. Ensure alignment of the data governance effort to the organization.

Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following statements is TRUE for point-to-point microwave transmissions?
A. They are not subject to interception due to encryption.
B. Interception only depends on signal strength.
C. They are too highly multiplexed for meaningful interception.
D. They are subject to interception by an antenna within proximity.
Answer: (SHOW ANSWER)

NEW QUESTION: 82
An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?
A. Elliptic Curve Cryptography (ECC) algorithm
B. Rivest-Shamir-Adleman (RSA) algorithm
C. Diffle-Hellman (DH) algorithm
D. Digital Signature algorithm (DSA)
Answer: (SHOW ANSWER)

NEW QUESTION: 83
What security risk does the role-based access approach mitigate MOST effectively?
A. Lack of system administrator activity monitoring
B. Segregation of duties conflicts within business applications
C. Inappropriate access requests
D. Excessive access rights to systems and data
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which of the following is the MOST appropriate action when reusing media that contains sensitive data?
A. Encrypt
B. Sanitize
C. Erase
D. Degauss
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Why is a system's criticality classification important in large organizations?
A. It allows for clear systems status communications to executive management.
B. It provides for easier determination of ownership, reducing confusion as to the status of the asset.

C. It provides for proper prioritization and scheduling of security and maintenance tasks.
D. It reduces critical system support workload and reduces the time required to apply patches.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
Physical assets defined in an organization's Business Impact Analysis (BIA) could include which of the following?
A. Cloud-based applications
B. Disaster Recovery (DR) line-item revenues
C. Supplies kept off-site at a remote facility
D. Personal belongings of organizational staff members
Answer: (SHOW ANSWER)

NEW QUESTION: 87
In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?
A. Reduced risk to internal systems.
B. Mitigate the risk associated with the exposed server.
C. Prepare the server for potential attacks.
D. Bypass the need for a firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following controls is the FIRST step in protecting privacy in an information system?
A. Data Storage
B. Data Encryption
C. Data Redaction
D. Data Minimization
Answer: (SHOW ANSWER)

NEW QUESTION: 89
What is the PRIMARY role of a scrum master in agile development?
A. To choose the primary development language
B. To match the software requirements to the delivery plan
C. To choose the integrated development environment
D. To project manage the software delivery
Answer: (SHOW ANSWER)

NEW QUESTION: 90
By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

A. Lock bumping
B. Lock bricking
C. Lock picking
D. Lock pinging
Answer: (SHOW ANSWER)

NEW QUESTION: 91
A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?
A. Insurance against litigation following a disaster
B. Guaranteed recovery of all business functions
C. Protection from loss of organization resources
D. Minimization of the need decision making during a crisis
Answer: (SHOW ANSWER)

NEW QUESTION: 92
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 6
C. Layer 5
D. Layer 4
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?
A. undergo a security assessment as part of authorization process
B. establish policies and procedures on system and services acquisition
C. harden the hosting server, and perform hosting and application vulnerability scans
D. establish a risk management strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Copyright provides protection for which of the following?
A. A particular expression of an idea
B. Discoveries of natural phenomena
C. New and non-obvious inventions
D. Ideas expressed in literary works
Answer: (SHOW ANSWER)

NEW QUESTION: 95
A criminal organization is planning an attack on a government network. Which of the following is the MOST severe attack to the network availability?
A. Sensitive information is gathered on the network topology by attacker
B. Operator loses control of network devices to attacker
C. Network management communications is disrupted
D. Network is flooded with communication traffic by attacker
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which of the following is the BEST statement for a professional to include as port of businees continuity (BC) procedure?
A. A full data backup must be done based on the needs of the business.
B. An incremental data backup must be done upon management request.
C. In incremental data backup must be done after each system change.
D. A full data backup must be done upon management request.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
Which of the following is ensured when hashing files during chain of custody handling?
A. Availability
B. Accountability
C. Non-repudiation
D. Integrity
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Which of the following is applicable to a publicly held company concerned about information handling and storage requirement specific to the financial reporting?
A. International Organization for Standardization (ISO) 27001
B. Privacy Act of 1974
C. Clinger-Cohan Act of 1996

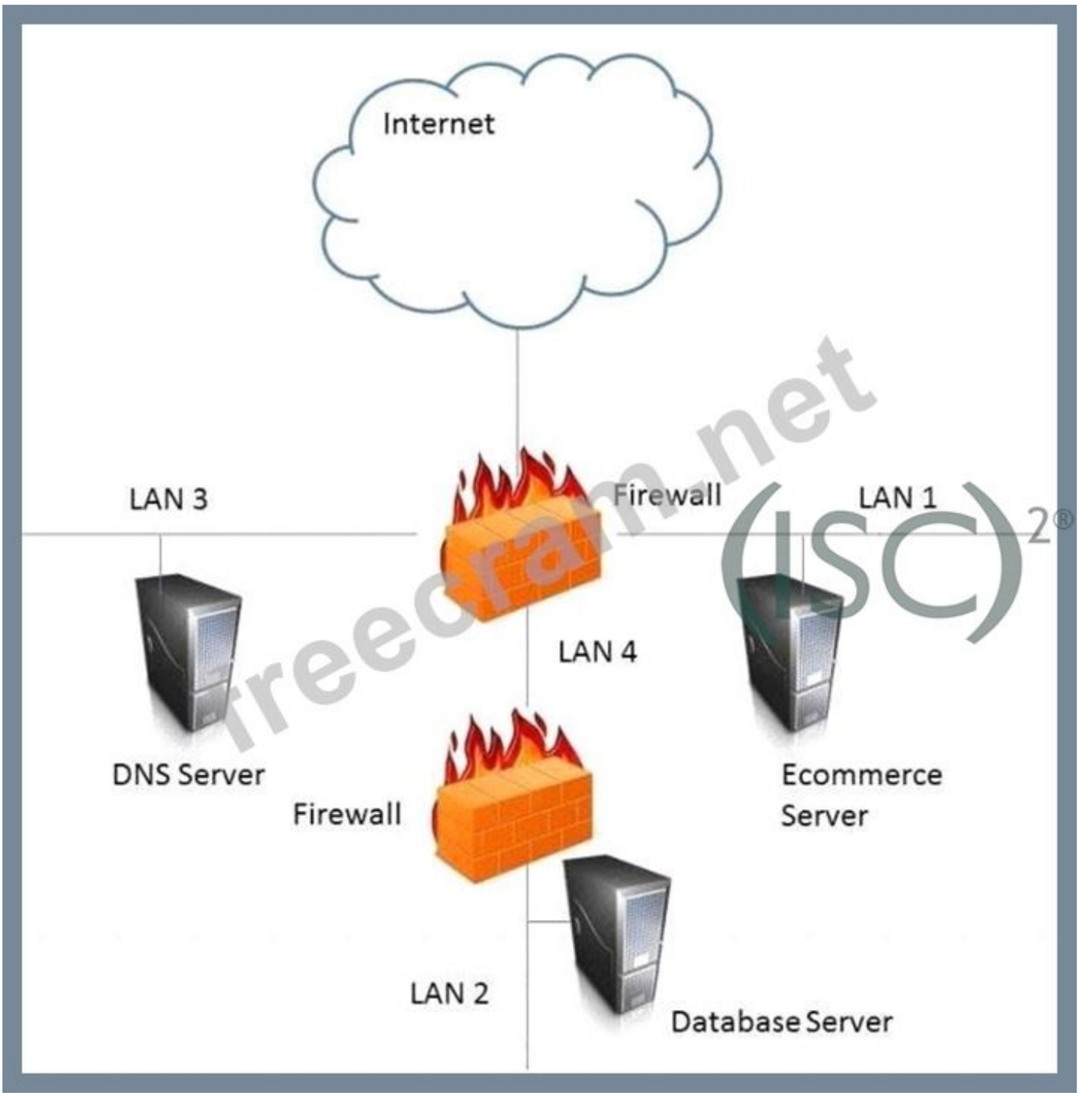
D. Sarbanes-Oxley (SOX) Act of 2002
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which of the following is the BEST countermeasure to brute force login attacks?
A. Decreasing the number of concurrent user sessions
B. Changing all canonical passwords
C. Restricting initial password delivery only in person
D. Introducing a delay after failed system access attempts
Answer: (SHOW ANSWER)

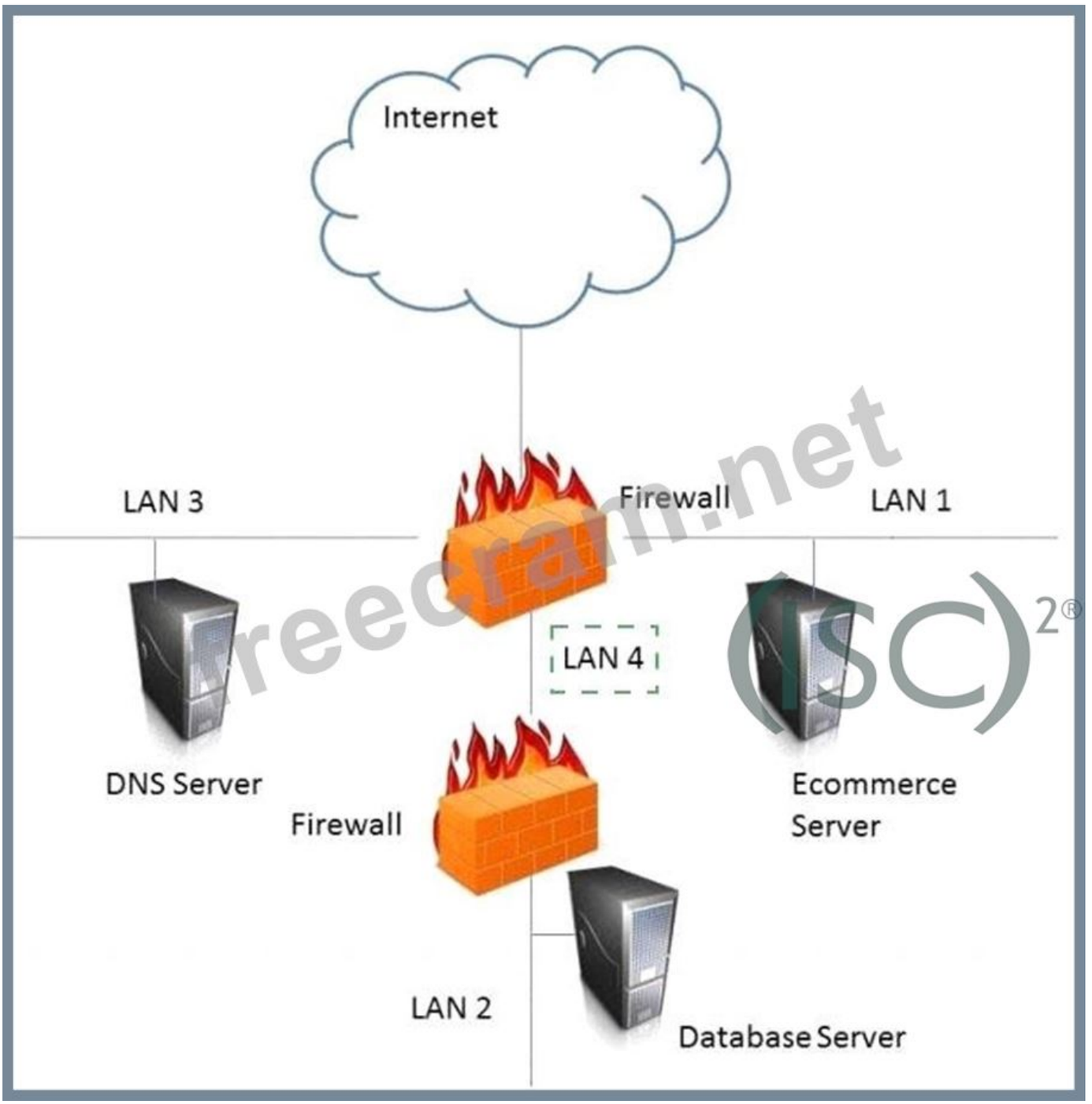
NEW QUESTION: 100
What is the PRIMARY difference between security policies and security procedures?
A. Policies are used to enforce violations, and procedures create penalties
B. Policies are generic in nature, and procedures contain operational details
C. Policies point to guidelines, and procedures are more contractual in nature
D. Policies are included in awareness training, and procedures give guidance
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Which of the following roles has the obligation to ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization?
A. Data Owner
B. Data User
C. Data Custodian
D. Data Creator
Answer: (SHOW ANSWER)

NEW QUESTION: 102
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?


Internet
LAN 3
Firewall
LAN 1
LAN 4
DNS Server
Firewall
Ecommerce Server
LAN 2
Database Server

Answer:



Explanation
LAN 4

NEW QUESTION: 103
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?
A. Addresses and protocols of network-based logs are analyzed.
B. Network-based systems cannot capture users logging into the console.
C. Properly handled network-based logs may be more reliable and valid.
D. Host-based system logging has files stored in multiple locations.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?
A. Approve the application that best meets security requirements.
B. Accept the risk on behalf of the organization.
C. Report findings to the business to determine security gaps.
D. Quantify the risk to the business for product selection.
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following is the MOST crucial for a successful audit plan?
A. Working with the system owner on new controls
B. Defining the scope of the audit to be performed
C. Acquiring evidence of systems that are not compliant
D. Identifying the security controls to be implemented
Answer: (SHOW ANSWER)

NEW QUESTION: 106
What is the MOST efficient way to secure a production program and its data?
A. Disable unused services and implement tunneling
B. Disable default accounts and implement access control lists (ACL)
C. Harden the application and encrypt the data
D. Harden the servers and backup the data
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?
A. Documentation, observation, and manual
B. Tactical, strategic, and financial
C. Standards, policies, and procedures

D. Management, operational, and technical
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Which of the following is the MOST important action regarding authentication?
A. Establishing audit controls
B. Enrolling in the system
C. Granting access rights
D. Obtaining executive authorization
Answer: (SHOW ANSWER)

NEW QUESTION: 109
An organization that has achieved a Capability Maturity model Integration (CMMI) level of 4 has done which of the following?
A. Addressed the causes of common process variance
B. Achieved optimized process performance
C. Addressed continuous innovative process improvement
D. Achieved predictable process performance
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which of the following MOST applies to session initiation protocal (SIP) security?
A. It leverages Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS).
B. It requires a Public Key Infrastructure (PKI).
C. It reuses security mechanisms derived from existing protocols.
D. It supports end-to-end security natively.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 111
In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of
A. systems integration.
B. change management.
C. risk management.
D. quality assurance.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
The use of private and public encryption keys is fundamental in the implementation of which of the following?
A. Secure Sockets Layer (SSL)

B. Diffie-Hellman algorithm
C. Message Digest 5 (MD5)
D. Advanced Encryption Standard (AES)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
Which of the following are effective countermeasures against passive network-layer attacks?
A. Encryption and security enabled applications
B. Federated security and authenticated access controls
C. Trusted software development and run time integrity controls
D. Enclave boundary protection and computing environment defense
Answer: A (LEAVE A REPLY)

NEW QUESTION: 114
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. Security Assertion Markup Language (SAML)
B. Extensible Markup Language (XML)
C. Standard Generalized Markup Language (SGML)
D. Transaction Authority Markup Language (XAML)
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following BEST describes a Protection Profile (PP)?
A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
B. A document that is used to develop an IT security product from its security requirements definition.
C. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).
D. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the
A. opportunity for device identity spoofing is eliminated.
B. storage devices are protected against availability attacks.
C. opportunity to sniff network traffic exists.

D. confidentiality of the traffic is protected.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which one of the following transmission media is MOST effective in preventing data interception?
A. Twisted-pair
B. Fiber optic
C. Coaxial cable
D. Microwave
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Which of the following methods can be used to achieve confidentiality and integrity for data in transit?
A. Multi-factor authentication
B. Federated identity management
C. Multiprotocol Label Switching (MPLS)
D. Internet Protocol Security (IPSec)
Answer: (SHOW ANSWER)

NEW QUESTION: 119
An organization implements a remote access server (RAS), Once users connect to the server, digital certificates are used to authenticate their identity. What type of extensible Authentication protocol (EAP) would the organization use during this authentication?
A. Lightweight Extensible Authentication Protocol (EAP)
B. Transport layer security (TLS)
C. Message Digest 5 (MD5)
D. Subscriber Identity Module (SIM)
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

A. Delete every file on each drive.
B. Destroy the partition table for each drive using the command line.
C. Degauss each drive individually.
D. Perform multiple passes on each drive using approved formatting methods.
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Who must approve modifications to an organization's production infrastructure configuration?

A. System operations
B. Change control board
C. Technical management
D. System users
Answer: (SHOW ANSWER)

NEW QUESTION: 122
Which of the following presents the PRIMARY concern to an organiztion when setting up a federated single sign-on (SSO) solution with another
A. defining the identity mapping scheme
B. Requesting Identity assertions from the partners domain
C. Having the resource provider query the Identity provider
D. Sending assertions to an identity provider
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which of the following methods MOST efficiently manages user accounts when using a third-party cloud-based application and directory solution?
A. Directory synchronization
B. Lightweight Directory Access Protocol (LDAP)
C. Cloud directory
D. Assurance framework
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which item below is a federated identity standard?
A. 802.11i
B. Security Assertion Markup Language (SAML)
C. Kerberos
D. Lightweight Directory Access Protocol (LDAP)
Answer: (SHOW ANSWER)

NEW QUESTION: 125
What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?
A. Determine business drivers
B. Review the security baseline configuration
C. Identify regulatory requirements
D. Conduct a risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 126
When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?
A. Only when controls are put in place
B. Only when assets are clearly defined
C. Only when standards are defined
D. Only procedures are defined
Answer: B (LEAVE A REPLY)

NEW QUESTION: 127
What is the second step in the identity and access provisioning lifecycle?
A. Review
B. Approval
C. Revocation
D. Provisioning
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which area of embedded devices are most commonly attacked?
A. Firmware
B. Physical Interface
C. Protocol
D. Application
Answer: (SHOW ANSWER)

NEW QUESTION: 129
What physical characteristic does a retinal scan biometric device measure?
A. The size, curvature, and shape of the retina
B. The pattern of light receptors at the back of the eye
C. The pattern of blood vessels at the back of the eye
D. The amount of light reflected by the retina

Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
What is the MAIN feature that onion routing networks offer?
A. Traceability
B. Resilience
C. Anonymity
D. Non-repudiation
Answer: (SHOW ANSWER)

NEW QUESTION: 131
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: (SHOW ANSWER)
Reference:
https://securityintelligence.com/dont-dwell-on-it-how-to-detect-a-breach-on-your-network-more-efficiently

NEW QUESTION: 132
A security consultant has been hired by a company to establish its vulnerability management program.
The consultant is now in the deployment phase. Which of the following tasks is part of this process?
A. Determine a budget and cost analysis for the program.
B. Educate and train key stakeholders.
C. Measure effectiveness of the program's stated goals.
D. Select and procure supporting technologies.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Which of the following authorization standards is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM)?
A. Open Authentication (OAUTH)
B. Terminal Access Control Access Control System Plus (TACACS+)
C. Security Assertion Markup Language (SAML)
D. Remote Authentication Dial-in User service (RADIUS)
Answer: (SHOW ANSWER)

NEW QUESTION: 134
The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?
A. A metadirectory
B. User self-service
C. Single Sign-On (SSO)
D. Two-factor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?
A. Establish a secure initial state
B. Interface with the Public Key Infrastructure (PKI)
C. Improve the quality of security software
D. Prevent Denial of Service (DoS) attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?
A. Logging and audit trail controls to enable forensic analysis
B. Security event alert triage done by analysts using a Security Information and Event Management (SIEM) system
C. Security incident response lessons learned procedures
D. Transactional controls focused on fraud prevention
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?
A. It uses a Subscriber Identity Module (SIM) for authentication.

B. The signal is difficult to read as it provides end-to-end encryption.
C. It uses encrypting techniques for all communications.
D. The radio spectrum is divided with multiple frequency carriers.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Although code using a specific program language may not be susceptible to a buffer overflow attack,
A. the graphical images used by the application could be susceptible.
B. most supporting application code is susceptible.
C. most calls to plug-in programs are susceptible.
D. the supporting virtual machine could be susceptible.
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Why are mobile devices sometimes difficult to investigate in a forensic examination?
A. They may have proprietary software installed to protect them.
B. They have password-based security at logon.
C. There are no forensic tools available for examination.
D. They may contain cryptographic protection.
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

A. Segregate the database into a small number of partitions each with a separate security level
B. Limit access to predefined queries
C. Reduce the number of people who have access to the system for statistical purposes
D. Implement Role Based Access Control (RBAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Which of the following is the MOST
A. Segmentation
B. Error correction
C. Virtual Local Area Network (VLAN) tagging
D. Compartmentalization
Answer: (SHOW ANSWER)

NEW QUESTION: 142

In the common criteria (CC) for information technology (IT) security evaluation, increasing Evaluation Assurance Levels (EAL) results in which of the following?
A. Increase in evaluated systems
B. Increased interoperability
C. Increased functionality
D. Increase in resource requirement
Answer: B (LEAVE A REPLY)

NEW QUESTION: 143
In a data classification scheme, the data is owned by the
A. end users
B. business managers
C. Information Technology (IT) managers
D. system security managers
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?
A. Authorized user control
B. Discretionary Access Control (DAC)
C. Access Control List (ACL)
D. Mandatory Access Control (MAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 145
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?
A. To create a high level DRP awareness among Information Technology (IT) staff
B. To validate backup sites' effectiveness
C. To find out what does not work and fix it
D. To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
Answer: B (LEAVE A REPLY)

NEW QUESTION: 146
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: (SHOW ANSWER)
Reference: https://en.wikipedia.org/wiki/Attribute-based_access_control

NEW QUESTION: 147
From a security perspective, which of the following assumptions MUST be made about input to an application?
A. It is verified
B. It is untrusted
C. It is tested
D. It is logged
Answer: (SHOW ANSWER)

NEW QUESTION: 148
A vulnerability test on an Information System (IS) is conducted to
A. exploit security weaknesses in the IS.
B. evaluate the effectiveness of security controls.
C. measure system performance on systems with weak security controls.
D. prepare for Disaster Recovery (DR) planning.
Answer: (SHOW ANSWER)

NEW QUESTION: 149
Who is ultimately responsible to ensure that information assets are categorized and adequate measures are taken to protect them?
A. Data Custodian
B. Chief Information Security Officer
C. Executive Management
D. Data/Information/Business Owners
Answer: (SHOW ANSWER)

NEW QUESTION: 150
In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?
A. An activation of the backup site
B. A full-scale simulation of an emergency and the subsequent response functions
C. A specific test by response teams of individual emergency response functions
D. A functional evacuation of personnel
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Which of the following combinations would MOST negatively affect availability?
A. Unauthorized transactions and denial of service attacks
B. Unauthorized transactions and outdated hardware

C. Denial of Service (DoS) attacks and outdated hardware
D. Fire and accidental changes to data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 152
For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?
A. System Security Architect
B. Data Owner
C. Security Requirements Analyst
D. Information Systems Security Officer
Answer: (SHOW ANSWER)

NEW QUESTION: 153
Which security architecture strategy could be applied to secure an operating system (OS) baseline for deployment within the corporate enterprise?
A. Principle of Secure Default
B. principle of Fail Secure
C. Principle of Least Privilege
D. Principle of Separation of Duty
Answer: (SHOW ANSWER)

NEW QUESTION: 154
In a financial institution, who has the responsibility for assigning the classification to a piece of information?
A. Originator or nominated owner of the information
B. Department head responsible for ensuring the protection of the information
C. Chief Financial Officer (CFO)
D. Chief Information Security Officer (CISO)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 155

What is the MOST critical factor to achieve the goals of a security program?
A. Executive management support
B. Capabilities of security resources
C. Budget approved for security resources
D. Effectiveness of security management
Answer: (SHOW ANSWER)

NEW QUESTION: 156
While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?
A. They should be inspected and sanitized following the organizational policy.
B. They should be recycled to save energy.
C. They should be recycled according to NIST SP 800-88.
D. They should be inspected and categorized properly to sell them for reuse.
Answer: (SHOW ANSWER)

NEW QUESTION: 157
The BEST method to mitigate the risk of a dictionary attack on a system is to
A. use a hardware token.
B. implement password history.
C. encrypt the access control list (ACL).
D. use complex passphrases.
Answer: (SHOW ANSWER)

NEW QUESTION: 158
An organization has developed a major application that has undergone accreditation testing. After receiving the results of the evaluation, what is the final step before the application can be accredited?
A. Approval of the System Security Plan (SSP)
B. Adoption of standardized policies and procedures
C. Remediation of vulnerabilities
D. Acceptance of risk by the authorizing official
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Data leakage of sensitive information is MOST often concealed by which of the following?
A. Secure Post Office Protocol (POP)
B. Secure Sockets Layer (SSL)
C. Wired Equivalent Privacy (WEP)
D. Secure Hash Algorithm (SHA)

Answer: (SHOW ANSWER)

NEW QUESTION: 160

Why is planning in Disaster Recovery (DR) an interactive process?

A. It identifies omissions in the plan

B. It details off-site storage plans

C. It defines the objectives of the plan

D. It forms part of the awareness process

Answer: (SHOW ANSWER)

NEW QUESTION: 161

Which is the MOST critical aspect of computer-generated evidence?

A. Relevancy

B. Integrity

C. Timeliness

D. Objectivity

Answer: (SHOW ANSWER)

NEW QUESTION: 162

Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

A. Authentication validation

B. Policy documentation review

C. Interface testing

D. Periodic log reviews

Answer: (SHOW ANSWER)

NEW QUESTION: 163

What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

A. Role-Based Access Control (RBAC)

B. Audit logs

C. Two-factor authentication

D. Application of least privilege

Answer: (SHOW ANSWER)

NEW QUESTION: 164

For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

A. Content data

B. User data

C. Alert data
D. Statistical data
Answer: (SHOW ANSWER)

NEW QUESTION: 165
What steps can be taken to prepare personally identifiable information (PII) for processing by a third party?
A. The personal information can be hashed and then the data can be sent to an outside processor.
B. The personal information should be maintained separately connected with a one-way reference.
C. It is not necessary to protect PII as long as it is in the hands of the provider.
D. A security agreement with a Cloud Service Provider (CSP) was required so there is no concern.
Answer: (SHOW ANSWER)

NEW QUESTION: 166
A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.
Which of the following is the BEST location?
A. On the top floor
B. In the basement
C. In the core of the building
D. In an exterior room with windows
Answer: (SHOW ANSWER)

NEW QUESTION: 167
An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is
A. organization policy.
B. management feedback.

C. industry laws and regulations.
D. industry best practices.
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?
A. identity provisioning
B. multi-factor authentication (MFA)
C. user access review
D. access recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 169
Which of the following would be the FIRST step to take when implementing a patch management program?
A. Create a system inventory.
B. Perform automatic deployment of patches.
C. Prioritize vulnerability remediation.
D. Monitor for vulnerabilities and threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

A. Perform the change, but create a change ticket regardless to ensure there is complete traceability.
B. Ignore the request and do not perform the change.
C. Inform the audit committee or internal audit directly using the corporate whistleblower process.
D. Perform the change as requested, and rely on the next audit to detect and report the situation.
Answer: C (LEAVE A REPLY)

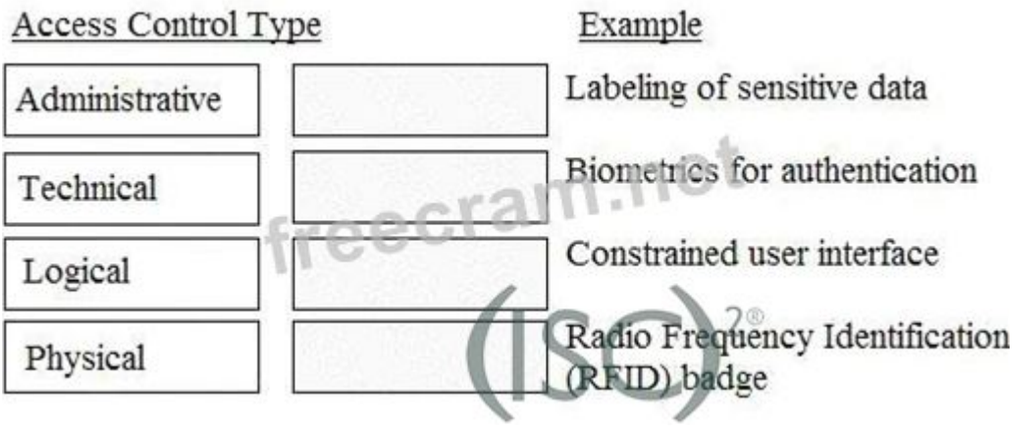
NEW QUESTION: 171
What are the steps of a risk assessment?
A. identification, analysis, evaluation
B. analysis, evaluation, mitigation
C. classification, identification, risk management
D. identification, evaluation, mitigation
Answer: (SHOW ANSWER)
Explanation

Section: Security Assessment and Testing

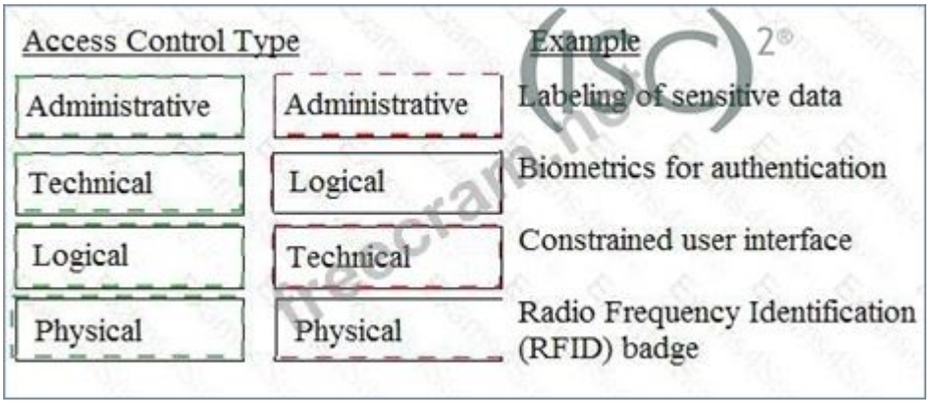
NEW QUESTION: 172

Match the access control type to the example of the control type.

Drag each access control type net to its corresponding example.



Answer:



Explanation

Administrative - labeling of sensitive data

Technical - Constrained user interface

Logical - Biometrics for authentication

Physical - Radio Frequency Identification 9RFID) badge

NEW QUESTION: 173

In Business Continuity Planning (BCP), what is the importance of documenting business processes?

A. Provides an understanding of the organization's interdependencies

B. Defines who will perform which functions during a disaster or emergency

C. Establishes and adopts ongoing testing and maintenance strategies

D. Provides senior management with decision-making tools

Answer: (SHOW ANSWER)

NEW QUESTION: 174

The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

A. retain its current EAL rating.

B. require recertification.

C. reduce the product to EAL 3.

D. require an update of the Protection Profile (PP).

Answer: (SHOW ANSWER)

NEW QUESTION: 175

Access to which of the following is required to validate web session management?

A. Log timestamp

B. Live session traffic

C. Test scripts

D. Session state variables

Answer: B (LEAVE A REPLY)

NEW QUESTION: 176

Which of the following is considered a secure coding practice?

A. Use new code for common tasks

B. Use checksums to verify the integrity of libraries

C. Use dynamic execution functions to pass user supplied data

D. Use concurrent access for shared variables and resources

Answer: (SHOW ANSWER)

NEW QUESTION: 177

The 802.1x standard provides a framework for what?

A. Network authentication for only wireless networks

B. Wireless encryption using the Advanced Encryption Standard (AES)

C. Wireless network encryption using Secure Sockets Layer (SSL)

D. Network authentication for wired and wireless networks

Answer: (SHOW ANSWER)

NEW QUESTION: 178

Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?

A. Cyclic redundancy check (CRC)

B. Data at rest encryption

C. Integrity checking software

D. Configuration Management

Answer: (SHOW ANSWER)

NEW QUESTION: 179
A project requires the use of en authentication mechanism where playback must be protected and plaintext secret must be used. Which of the following should be used?
A. Secure Hash Algorithm (SHA)
B. Password Authentication Protocol (PAP)
C. Challenge Handshake Authentication Protocol (CHAP)
D. Extensible Authentication Protocol (EAP)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 180
Which of the following is the GREATEST security risk associated with the user of identity as a service (IDaaS) when an organization its own software?

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

NEW QUESTION: 181
Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?
A. Data Link
B. Network
C. Transport
D. Session
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
Rank the Hypertext Transfer protocol (HTTP) authentication types shows below in order of relative strength.
Drag the authentication type on the correct positions on the right according to strength from weakest to strongest.

Answer:

Explanation

NEW QUESTION: 183

Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

A. Background checks, data encryption, web proxies

B. Least privilege access, Data Loss Protection (DLP), physical access controls

C. Staff vetting, least privilege access, Data Loss Protection (DLP)

D. Data Loss Protection (DIP), firewalls, data classification

Answer: (SHOW ANSWER)

NEW QUESTION: 184

Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Passwords are passed in cleartext

B. Unsalted hashes are passed over the network

C. The authentication session can be replayed

D. Authorizations are not included in the server response

Answer: (SHOW ANSWER)

NEW QUESTION: 185
Why are mobile devices something difficult to investigate in a forensic examinition?
A. They have password-based security at logon.
B. They may contain cryptographic protection.
C. There are no forensics tools available for examination.
D. They may have proprietary software installed to protect them.
Answer: (SHOW ANSWER)

NEW QUESTION: 186
Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device Which has stolen?
A. Whole device encryption with key escrow
B. Virtual Private Network (VPN) with traffic encryption
C. Mobile Device Management (MDMJ with device wipe
D. Mobile device tracking with geolocation
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Which of the following represents the GREATEST risk to data confidentiality?
A. Backup tapes are generated unencrypted
B. Security awareness training is not completed
C. Users have administrative privileges
D. Network redundancies are not implemented
Answer: (SHOW ANSWER)

NEW QUESTION: 188
Which of the following is the MOST important activity an organization performs to ensure that securiy is part of the overall organization culture?
A. Work with senior management to meet business goals.
B. Perform formal reviews of security Incidents.
C. Ensue security policies are issued to all employees
D. Manage a program of security audits.
Answer: (SHOW ANSWER)

NEW QUESTION: 189
A control to protect from a Denial-of-Service (DoS) attach has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?
A. 100%
B. 75%
C. 25%
D. 50%

Answer: (SHOW ANSWER)

NEW QUESTION: 190

What does the Maximum Tolerable Downtime (MTD) determine?

A. The estimated period of time a business can remain interrupted beyond which it risks never recovering

B. The fixed length of time in a DR process before redundant systems are engaged

C. The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning

D. The estimated period of time a business critical database can remain down before customers are affected.

Answer: (SHOW ANSWER)

NEW QUESTION: 191

Which of the following is the FIRST step in the incident response process?

A. Investigate all symptoms to confirm the incident

B. Isolate and contain the system involved

C. Determine the cause of the incident

D. Disconnect the system involved from the network

Answer: (SHOW ANSWER)

NEW QUESTION: 192

Which of the following should be included a hardware retention policy?

A. The use of encryption technology to encrypt sensitive data prior to retention

B. Retention of all sensitive data on media and hardware

C. A plan to retain date required only for business purposes and a retention schedule

D. Retention of data for only one week and outsourcing the retention to a third-party vendor

Answer: (SHOW ANSWER)

NEW QUESTION: 193

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

A. Asset Management, Business Environment, Governance and Risk Assessment

B. Recovery Planning, Improvements and Communications

C. Access Control, Awareness and Training, Data Security and Maintenance

D. Anomalies and Events, Security Continuous Monitoring and Detection Processes

Answer: (SHOW ANSWER)

NEW QUESTION: 194

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR).
This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?
A. Block access to the offices immediately.
B. Revoke access temporarily.
C. Monitor account usage temporarily.
D. Block user access and delete user account after six months.
Answer: (SHOW ANSWER)

NEW QUESTION: 195
Which of the following is MOST important when deploying digital certificates?
A. Use a third-party Certificate Authority (CA)
B. Validate compliance with X.509 digital certificate standards
C. Establish a certificate life cycle management framework
D. Use no less than 256-bit strength encryption when creating a certificate
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Which of the following assures that rules are followed in an identity management architecture?
A. Digital signature
B. Policy decision point
C. Policy database
D. Policy enforcement point
Answer: (SHOW ANSWER)

NEW QUESTION: 197
Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?
A. Mandatory Access Control (MAC) procedures
B. Discretionary Access Control (DAC) procedures
C. Segregation of duties

D. Data link encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 198
The goal of a Business Impact Analysis (BIA) is to determine which of the following?
A. Which security measures should be implemented
B. Cost effectiveness of installing software security patches
C. Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
D. Cost effectiveness of business recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 199
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: (SHOW ANSWER)
Reference: http://ssae16.businesscatalyst.com/SSAE16_reports.html

NEW QUESTION: 200
Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

A. Document Object Model (DOM) trees
B. Web Interface Definition Language (IDL)
C. Cross Origin Resource Sharing (CORS)
D. WebSockets
Answer: (SHOW ANSWER)

NEW QUESTION: 201
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?
A. Internet Mail Access Protocol
B. Transport Layer Security (TLS)
C. Lightweight Directory Access Protocol (LDAP)
D. Security Assertion Markup Language (SAML)
Answer: (SHOW ANSWER)

NEW QUESTION: 202
Which of the following initiates the systems recovery phase of a disaster recovery plan?

A. Evacuating the disaster site
B. Assessing the extent of damage following the disaster
C. Activating the organization's hot site
D. Issuing a formal disaster declaration
Answer: (SHOW ANSWER)

NEW QUESTION: 203
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The effectiveness of the security program can PRIMARILY be measured through
A. risk elimination.
B. audit requirements.
C. customer satisfaction.
D. audit findings.
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Which of the following is MOST appropriate for protecting confidentially of data stored on a hard drive?
A. Advanced Encryption Standard (AES)
B. Triple Data Encryption Standard (3DES)
C. Message Digest 5 (MD5)
D. Secure Hash Algorithm 2(SHA-2)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 205
Which of the following is the primary advantage of segmenting Virtual Machines (VM) using physical networks?
A. Simplicity of network configuration and network redundancy
B. Simplicity of network configuration and network monitoring
C. Removes the need for dedicated virtual security controls
D. Removes the need for decentralized management solutions
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which of the following is PRIMARILY adopted for ensuring the integrity of information is preserved?
A. One-way encryption
B. Transport Layer Security (TLS)

C. Data at rest protection
D. Role Based Access Control (RBAC)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 207
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?
A. ISO/IEC 20000
B. International Organization for Standardization (ISO) 27000 family
C. Payment Card Industry Data Security Standard (PCIDSS)
D. Information Technology Infrastructure Library (ITIL)
Answer: (SHOW ANSWER)

NEW QUESTION: 208
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?
A. Application layer
B. Session layer
C. Link layer
D. Physical layer
Answer: (SHOW ANSWER)

NEW QUESTION: 209
What is the BEST way to establish identity over the internet?
A. Remote user authentication via Simple Object Access Protocol (SOAP)
B. Internet Mail Access Protocol (IMAP) with Triple Data Encryption Standard (3DES)
C. Challenge Handshake Authentication Protocol (CHAP) and strong passwords
D. Remote Authentication Dial-In User Service (RADIUS) server with hardware tokens
Answer: (SHOW ANSWER)

NEW QUESTION: 210
Mandatory Access Controls (MAC) are based on:
A. data labels and user access permissions
B. security classification and security clearance
C. data segmentation and data classification
D. user roles and data encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 211
Which of the following is considered the last line defense in regard to a Governance, Risk managements, and compliance (GRC) program?

A. Internal controls
B. Internal audit
C. Risk management
D. Board review
Answer: (SHOW ANSWER)

NEW QUESTION: 212
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?
A. Production Operations
B. Development and Deployment
C. Utilization Support
D. Requirements Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Which of the following is the best practice for testing a Business Continuity Plan (BCP)?
A. Test before the IT Audit
B. Test after implementation of system patches
C. Test after installation of security patches
D. Test when environment changes
Answer: (SHOW ANSWER)

NEW QUESTION: 214
In a basic SYN flood attack, what is the attacker attempting to achieve?
A. Set the threshold to zero for a given service
B. Exceed the threshold limit of the connection queue for a given service
C. Flush the register stack, allowing hijacking of the root account
D. Cause the buffer to overflow, allowing root access
Answer: (SHOW ANSWER)

NEW QUESTION: 215

Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

A. Applications' critically and downtime tolerance

B. Budget constraints and requirements

C. Cost/benefit analysis and business objectives

D. Hardware and software compatibility issues

Answer: (SHOW ANSWER)

NEW QUESTION: 216

What is the PRIMARY advantage of using automated application security testing tools?

A. Large amounts of code can be tested using fewer resources.

B. Detailed testing of code functions can be performed.

C. The application will fail less when tested using these tools.

D. The application can be protected in the production environment.

Answer: (SHOW ANSWER)

NEW QUESTION: 217

Who is accountable for the information within an Information System (IS)?

A. Security manager

B. System owner

C. Data owner

D. Data processor

Answer: B (LEAVE A REPLY)

Explanation

Section: Security Operations

NEW QUESTION: 218

Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

A. Delayed revocation or destruction of credentials

B. Modification of Certificate Revocation List

C. Token use after decommissioning

D. Unauthorized renewal or re-issuance

Answer: (SHOW ANSWER)

NEW QUESTION: 219

Which of the following BEST describes the responsibilities of data owner?

A. Determining the impact the information has on the mission of the organization

B. Maintaining fundamental data availability, including data storage and archiving

C. Ensuring accessibility to appropriate users, maintaining appropriate levels of data security

D. Ensuing Quality and validation trough periodic audits for ongoing data integrity

Answer: (SHOW ANSWER)

NEW QUESTION: 220

What balance MUST be considered when web application developers determine how information application error message should be constructed?

A. Performance versus user satisfaction

B. Confidentially versus integrity

C. Risk versus benefit

D. Availability versus auditability

Answer: (SHOW ANSWER)

NEW QUESTION: 221

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. Procure

D. Deploy

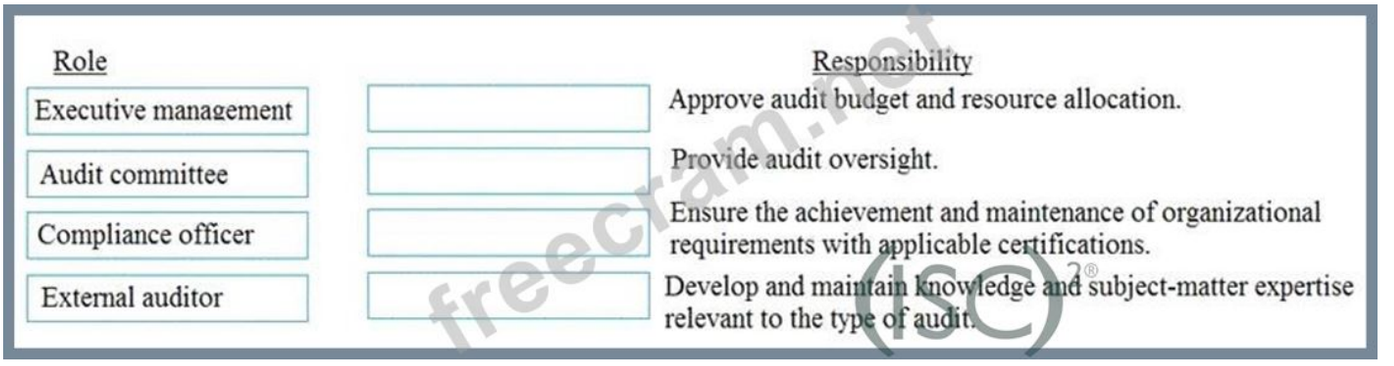
Answer: (SHOW ANSWER)

NEW QUESTION: 222

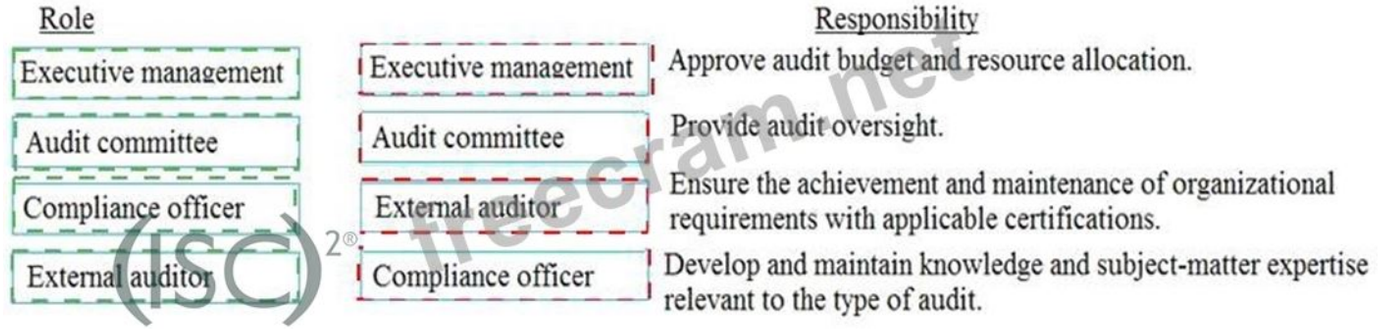
Match the functional roles in an external audit to their responsibilities.

Drag each role on the left to its corresponding responsibility on the right.

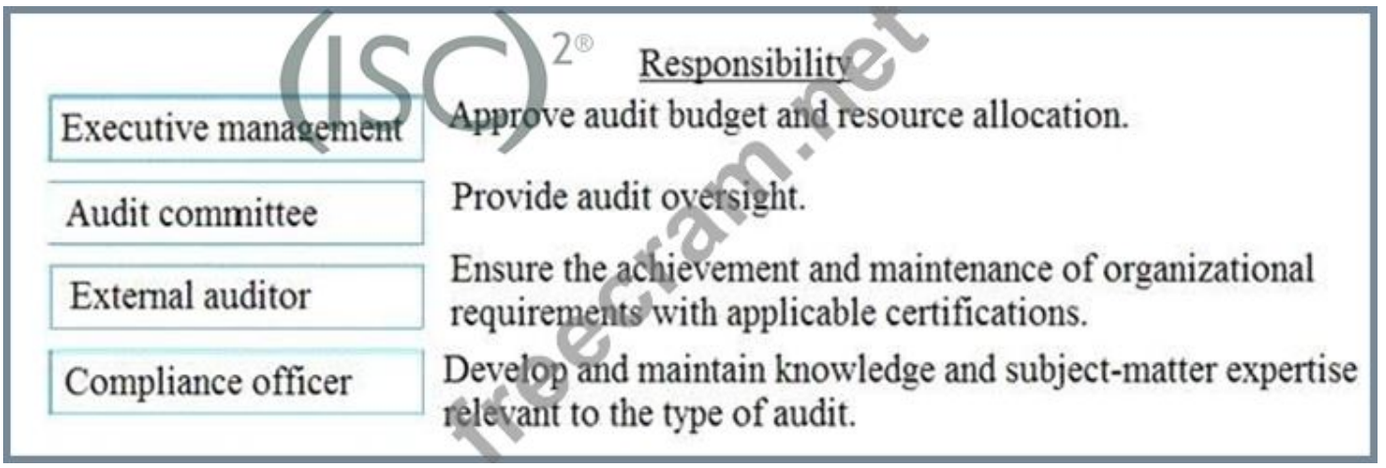
Select and Place:



Answer:



Explanation



NEW QUESTION: 223
Which one of the following is an advantage of an effective release control strategy form a configuration control standpoint?
A. Enforces backward compatibility between releases
B. Allows for future enhancements to existing features
C. Ensures that a trace for all deliverables is maintained and auditable
D. Ensures that there is no loss of functionality between releases
Answer: C (LEAVE A REPLY)

NEW QUESTION: 224
An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?
A. Inadequate cost modeling
B. Absence of a Business Intelligence (BI) solution
C. Insufficient Service Level Agreement (SLA)
D. Improper deployment of the Service-Oriented Architecture (SOA)
Answer: (SHOW ANSWER)

NEW QUESTION: 225
Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?
A. Lack of data access controls
B. Ineffective identity management controls
C. Ineffective data classification
D. Lack of Data Loss Prevention (DLP) tools
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Which of the following is a characteristic of a challenge/respones authentication process?
A. Presenting distorted graphics of text for authentication

B. Using a password history blacklist
C. Transmitting a hash based on the user
D. Requiring the use of non-consecutive numeric characters
Answer: (SHOW ANSWER)

NEW QUESTION: 227
An organization plan on purchasing a custom software product developed by a small vendor to support its business model. Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?
A. Right to request an independent review of the software source code
B. Due diligence form requesting statements of compliance with security requirements
C. A source code escrow clause
D. Access to the technical documentation
Answer: (SHOW ANSWER)

NEW QUESTION: 228
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

Answer:

Explanation

NEW QUESTION: 229

Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

A. Acquisition, Measurement, Configuration Management, Production, Operation, Support

B. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

C. Concept, Development, Production, Utilization, Support, Retirement

D. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation

Answer: (SHOW ANSWER)

NEW QUESTION: 230

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 hubs.

C. The network's firewall does not allow sniffing.

D. The network is connected using switches.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 231

When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

A. Incident likelihood

B. Countermeasure effectiveness

C. Type of potential loss

D. Information ownership

Answer: (SHOW ANSWER)

NEW QUESTION: 232
Which of the following will help identify the source internet protocol (IP) address of malware being exected on a computer?
A. Display the Address Resolution Protocol (APP) table.
B. List of running processes
C. Display Transmission Control Protocol/Internet Protocol (TCP/IP) network configuration information.
D. List of open network connections
Answer: (SHOW ANSWER)

NEW QUESTION: 233
What is the PRIMARY goal for using Domain Name System Security Extensions (DNSSEC) to sign records?
A. Integrity
B. Confidentiality
C. Accountability
D. Availability
Answer: (SHOW ANSWER)

NEW QUESTION: 234
A large corporation is looking for a solution to automate access based on where the request is coming from, who the user is, what device they are connecting with, and what and time of day they are attempting this access. What type of solution would suit their needs?
A. Discretionary Access Control (DAC)
B. Mandatory Access Control (MAC)
C. Role Based Access Control (RBAC)
D. Network Access Control (NAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 235
Which one of the following considerations has the LEAST impact when considering transmission security?
A. Network availability
B. Network bandwidth
C. Node locations
D. Data integrity
Answer: (SHOW ANSWER)

NEW QUESTION: 236
The adoption of an enterprise-wide business continuilty program requires Which of the folllowing?

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

NEW QUESTION: 237
At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?
A. Application Layer
B. Data-Link Layer
C. Network Layer
D. Transport Layer
Answer: (SHOW ANSWER)

NEW QUESTION: 238
Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?
A. Hashing the data before encryption
B. Compressing the data after encryption
C. Hashing the data after encryption
D. Compressing the data before encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 239
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Following best practice, where should the permitted access for each department and job classification combination be specified?
A. Human resource standards
B. Security standards
C. Security procedures
D. Human resource policy
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Which of the following is a characteristic of an internal audit?

A. An internal audit is typically shorter in duration than an external audit.
B. Management is responsible for reading and acting upon the internal audit results
C. The internal audit schedule is published to the organization well in advance.
D. The internal auditor reports to the Information Technology (IT) department
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Which of the following command line tools can be used in the reconnaisance phase of a network vulnerability assessment?
A. ifconfig
B. dig
C. nbtstat
D. ipconfig
Answer: B (LEAVE A REPLY)

NEW QUESTION: 242
Which of the following is a common characteristic of privacy?
A. Notice to the subject of the existence of a database containing relevant credit card data
B. Process for the subject to inspect and correct personal data on-site
C. Database requirements for integration of privacy data
D. Provision for maintaining an audit trail of access to the private data
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Which of the following is mobile device remote fingerprinting?
A. Storing information about a remote device in a cookie file
B. Retrieving the serial number of the mobile device
C. Identifying a device based on common characteristics shared by all devices of a certain type
D. Installing an application to retrieve common characteristics of the device
Answer: (SHOW ANSWER)

NEW QUESTION: 244

The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

A. Input validation

B. Device encryption

C. Application authentication

D. Digital signing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 245

Which programming methodology allows a programmer to use pre-determined blocks of code end consequently reducing development time and programming costs?

A. Assembly language

B. Blocked algorithm

C. Application security

D. Object oriented

Answer: (SHOW ANSWER)

NEW QUESTION: 246

Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A. Password requirements are simplified.

B. Risk associated with orphan accounts is reduced.

C. Data confidentiality is increased.

D. Segregation of duties is automatically enforced.

Answer: (SHOW ANSWER)

NEW QUESTION: 247

Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

A. Two-factor authentication

B. Passwords with alpha-numeric and special characters

C. Timed sessions and Secure Socket Layer (SSL)

D. Digital certificates and hardware tokens

Answer: (SHOW ANSWER)

NEW QUESTION: 248

What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

A. Inference

B. Signature

C. Induction

D. Heuristic
Answer: (SHOW ANSWER)

NEW QUESTION: 249
A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results.
What should be implemented to BEST
A. System performance monitoring application
B. Configuration Management Database (CMDB)
C. Configuration Management Plan (CMP)
D. Source code repository
Answer: (SHOW ANSWER)

NEW QUESTION: 250
Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?
A. Buffer division
B. Memory review
C. Code review
D. Message division
Answer: (SHOW ANSWER)

NEW QUESTION: 251
When using Security Assertion markup language (SAML), it is assumed that the principal subject
A. is on a system that supports remote authorization.
B. accepts persistent cookies from the system.
C. enrolls with at least one identity provider.
D. allows Secure Sockets Layer (SSL) for data exchanges.
Answer: (SHOW ANSWER)

NEW QUESTION: 252
What is the foundation of cryptographic functions?
A. Cipher
B. Entropy
C. Hash
D. Encryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 253
Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

A. Simultaneous connection to other networks
B. Remote users with administrative rights
C. Users with Internet Protocol (IP) addressing conflicts
D. VPN bandwidth
Answer: (SHOW ANSWER)

NEW QUESTION: 254
When building a data classification scheme, which of the following is the PRIMARY concern?
A. Cost effectiveness
B. Purpose
C. Authenticity
D. Availability
Answer: C (LEAVE A REPLY)

NEW QUESTION: 255
What is the purpose of an Internet Protocol (IP) spoofing attack?
A. To disguise the destination address from a target's IP filtering devices
B. To intercept network traffic without authorization
C. To convince a system that it is communicating with a known entity
D. To send excessive amounts of data to a process, making it unpredictable
Answer: (SHOW ANSWER)

NEW QUESTION: 256
Which of the following is the MOST important activity an organization performs to ensure that security is part of the overall organization culture?
A. Perform formal reviews of security incidents.
B. Work with senior management to meet business goals.
C. Ensure security policies are issued to all employees.
D. Manage a program of security audits.
Answer: (SHOW ANSWER)
Reference: https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

NEW QUESTION: 257

Which of the following is a network intrusion detection technique?

A. Statistical anomaly

B. Perimeter intrusion

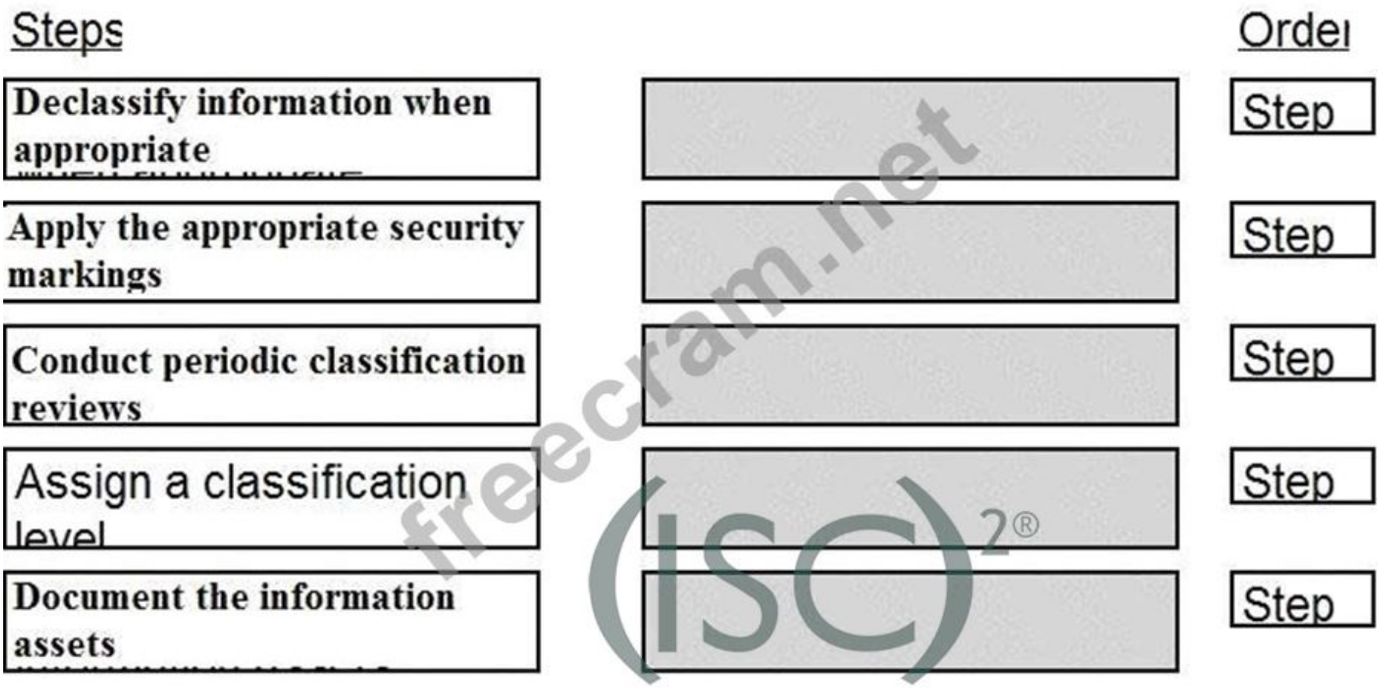
C. Network spoofing

D. Port scanning

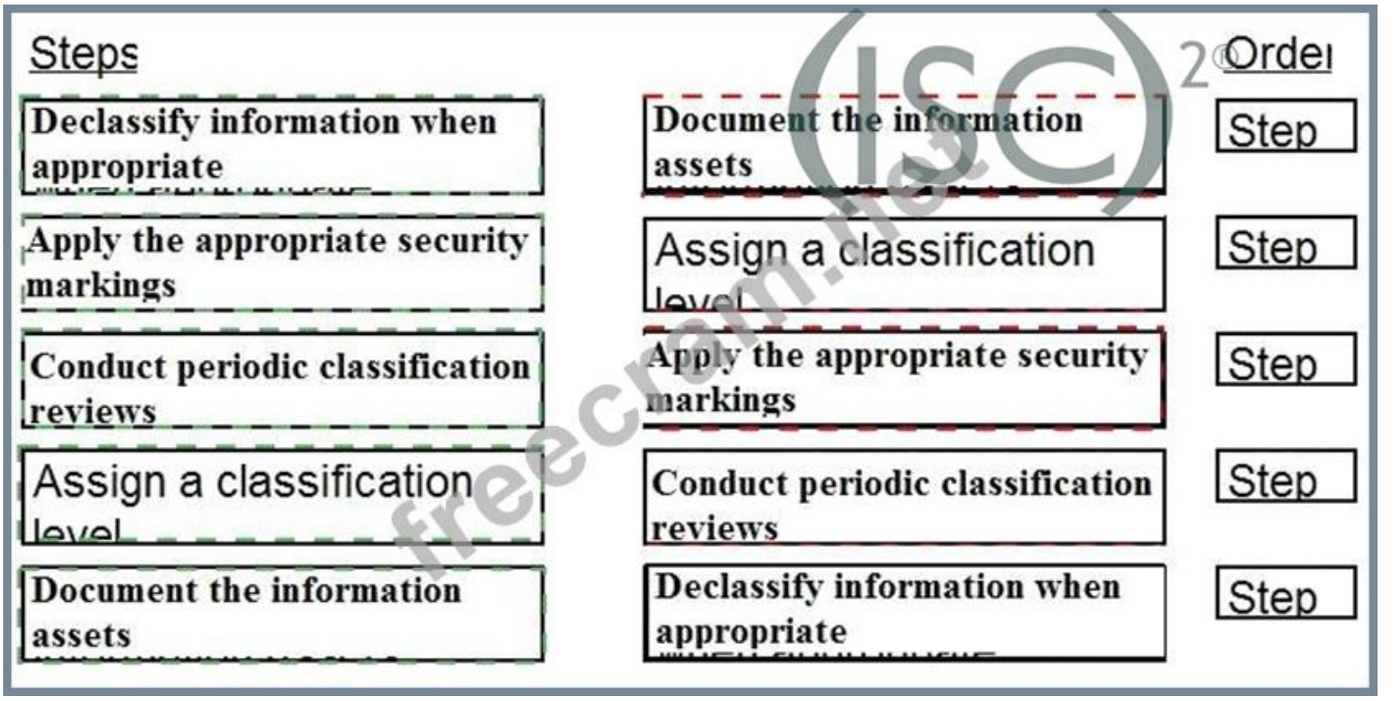
Answer: (SHOW ANSWER)

NEW QUESTION: 258

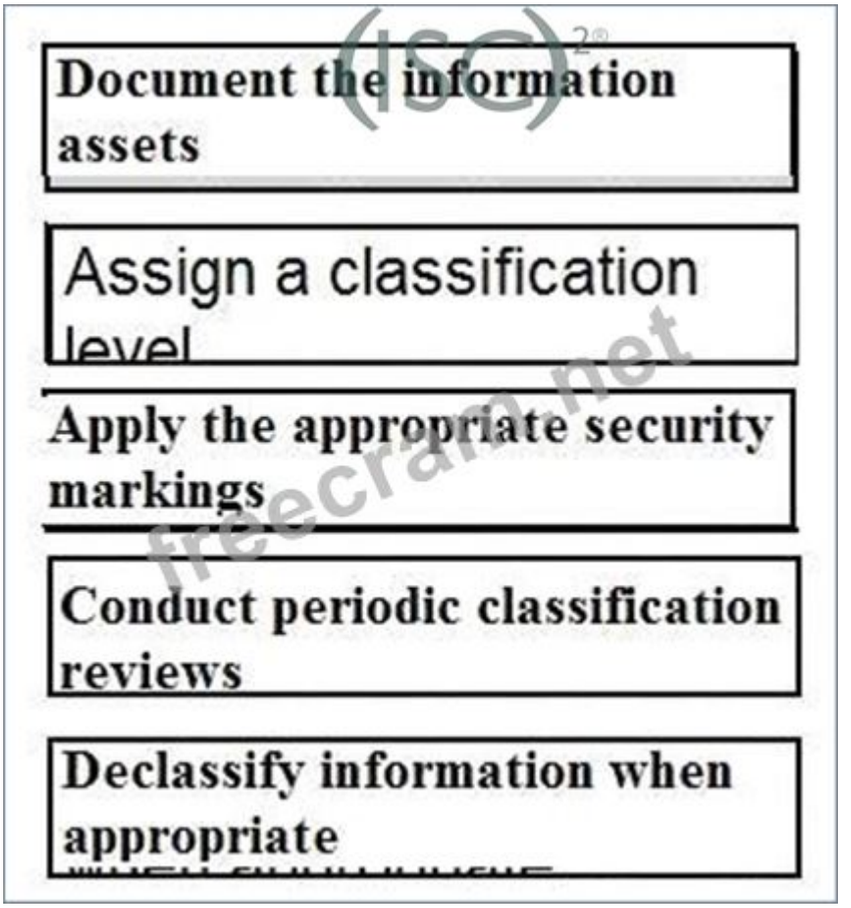
Place the following information classification steps in sequential order.



Answer:



Explanation



NEW QUESTION: 259

Which of the following media is least problematic with data remanence?

A. Dynamic Random Access Memory (DRAM)

B. Magnetic disk

C. Flash memory

D. Electrically Erasable Programming read-only Memory (EEPROM)

Answer: (SHOW ANSWER)

NEW QUESTION: 260

Additional padding may be added to the Encapsulating security protocol (ESP) trailer to provide which of the following?

A. protection ao>ainst replay attack

B. Data origin authentication

C. Partial traffic flow confidentiality

D. Access control

Answer: (SHOW ANSWER)

NEW QUESTION: 261

Which of the following is the MOST important security goal when performing application interface testing?

A. Examine error conditions related to external interfaces to prevent application details leakage
B. Confirm that all platforms are supported and function properly
C. Evaluate whether systems or components pass data and control correctly to one another
D. Verify compatibility of software, hardware, and network connections
Answer: (SHOW ANSWER)

NEW QUESTION: 262
What Is the FIRST step for a digital investigator to perform when using best practices to collect digital evidence from a potential crime scene?
A. Confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims.
B. Consult the lead investigate to team the details of the case and required evidence.
C. Assure that grounding procedures have been followed to reduce the loss of digital data due to static electricity discharge.
D. Update the Basic Input Output System (BIOS) and Operating System (OS) of any tools used to assure evidence admissibility.
Answer: (SHOW ANSWER)

NEW QUESTION: 263
During an audit, the auditor finds evidence of potentially illegal activity. Which of the following is the MOST appropriate action to take?
A. Immediately call the police
B. Advise the person performing the illegal activity to cease and desist
C. Work with the client to resolve the issue internally
D. Work with the client to report the activity to the appropriate authority
Answer: (SHOW ANSWER)

NEW QUESTION: 264
Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?
A. Set up a BIOS and operating system password
B. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
C. Encrypt the virtual drive where confidential files can be stored
D. Encrypt the entire disk and delete contents after a set number of failed access attempts
Answer: (SHOW ANSWER)

NEW QUESTION: 265
Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?
A. Personal Identity Verification (PIV)

B. Asymmetric Card Authentication Key (CAK) challenge-response
C. Cardholder Unique Identifier (CHUID) authentication
D. Physical Access Control System (PACS) repeated attempt detection
Answer: (SHOW ANSWER)

NEW QUESTION: 266
Which of the following is MOST effective in detecting information hiding in Transmission Control Protocol/internet Protocol (TCP/IP) traffic?
A. Stateful inspection firewall
B. Application-level firewall
C. Packet-filter firewall
D. Content-filtering proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 267
Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for implementing network security?
A. Session encryption
B. Hashing digest
C. Peer authentication
D. Payload data encryption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 268
A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?
A. The inherent risk is greater than the residual risk.
B. The infrastructure budget can easily cover the upgrade costs.
C. The Annualized Loss Expectancy (ALE) approaches zero.
D. The expected loss from the risk exceeds mitigation costs.
Answer: (SHOW ANSWER)

NEW QUESTION: 269
When is a Business Continuity Plan (BCP) considered to be valid?
A. When it has been validated by all threat scenarios
B. When it has been validated by the board of directors
C. When it has been validated by the Business Continuity (BC) manager
D. When it has been validated by realistic exercises
Answer: (SHOW ANSWER)

NEW QUESTION: 270

Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

A. detect objects of a specific temperature independent of the background temperature.
B. increase the detected object temperature in relation to the background temperature.
C. automatically compensate for variance in background temperature.
D. reduce the detected object temperature in relation to the background temperature.
Answer: (SHOW ANSWER)

NEW QUESTION: 271
Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?
A. A strong breach notification process
B. Continuous monitoring of potential vulnerabilities
C. End-to-end data encryption for data in transit
D. Limited collection of individuals' confidential data
Answer: (SHOW ANSWER)

NEW QUESTION: 272
When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?
A. Mapping tools
B. Topology diagrams
C. Asset register
D. Ping testing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 273
A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established.
What MUST be considered or evaluated before performing the next step?
A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened

C. Removing the server from the network may prevent catching the intruder
D. Copying the contents of the hard drive to another storage device may damage the evidence
Answer: C (LEAVE A REPLY)
Explanation
Section: Security Operations

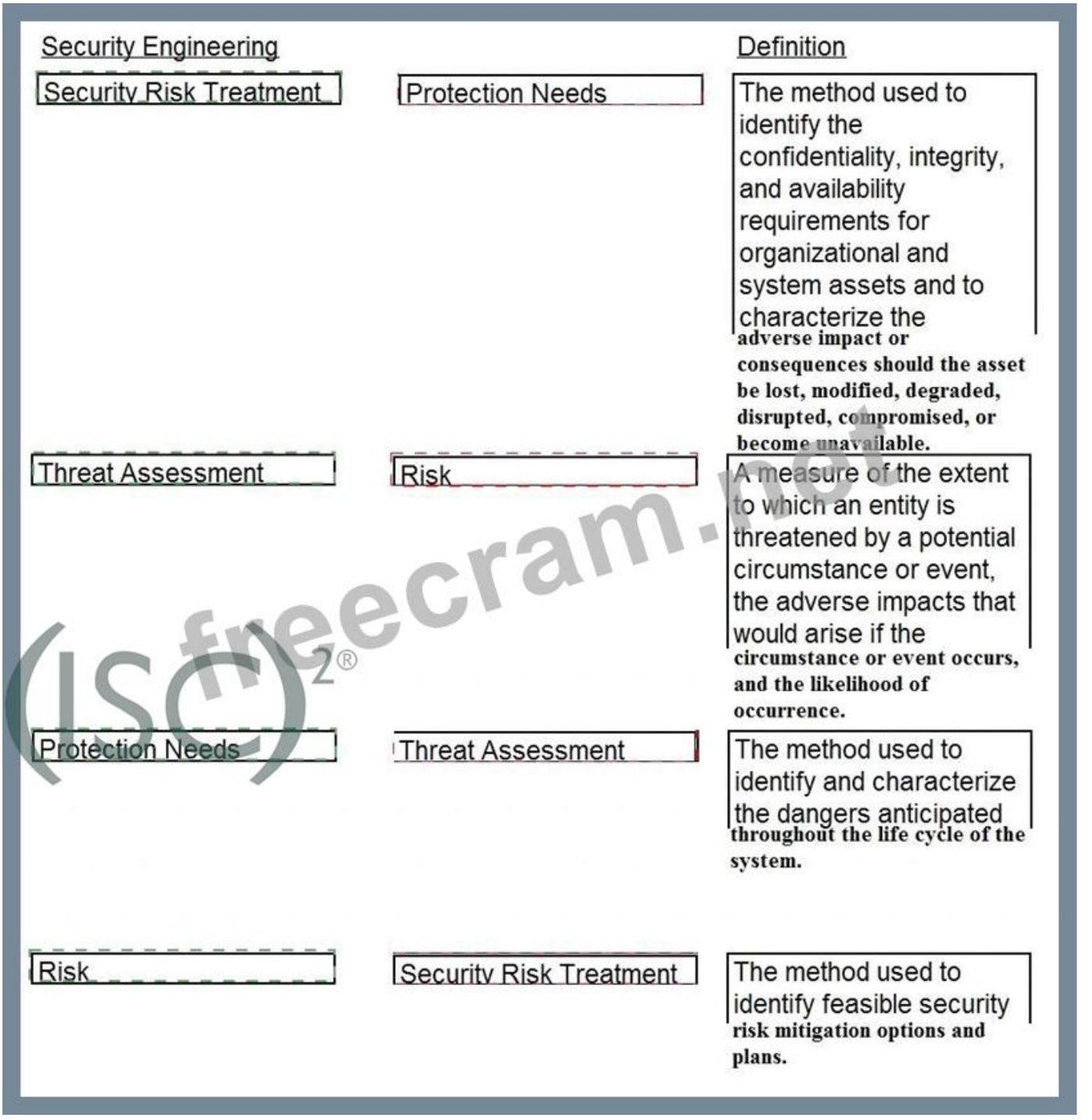
NEW QUESTION: 274
Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?
A. Secure card reader
B. Radio Frequency (RF) scanner
C. Intrusion Prevention System (IPS)
D. Anti-tampering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 275
Which of the following BEST describes the purpose of performing security certification?
A. To verify that system architecture and interconnections with other systems are effectively implemented
B. To formalize the confirmation of completed risk mitigation and risk analysis
C. To formalize the confirmation of compliance to security policies and standards
D. To identify system threats, vulnerabilities, and acceptable level of risk
Answer: (SHOW ANSWER)

NEW QUESTION: 276
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering		Definition
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs		The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk		The method used to identify feasible security **risk mitigation options and plans.**

Answer:



Explanation

	Definition
Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Threat Assessment	The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Security Risk Treatment	The method used to

Security Risk Treatment	The method used to identify feasible security **risk mitigation options and plans.**

NEW QUESTION: 277
Which of the following is an initial consideration when developing an information security management system?
A. Identify the contractual security obligations that apply to the organizations
B. Identify relevant legislative and regulatory compliance requirements
C. Identify the level of residual risk that is tolerable to management
D. Understand the value of the information assets
Answer: (SHOW ANSWER)

NEW QUESTION: 278
Why should Open Wab Application Secuirty Project (OWASP) Application Security Verification standards (ASVS) Level 1 be considered a MINIMUM level of protection for any wab application?
A. Securing applications at ASVS Level 1 provides adequate protection for sensitive data.
B. ASVS Level 1 ensures that applications are invulnerable to OWASP top 10 threats.
C. Most regulatory bodies consider ASVS Level 1 as a baseline set of controls for applications.
D. Opportunistic attackers will look for any easily exploitable vulnerable applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 279
What is the GREATEST challenge of an agent-based patch management solution?
A. The consistency of distributing patches to each participating computer
B. Time to gather vulnerability information about the computers in the program
C. Requires that software be installed, running, and managed on all participating computers
D. The significant amount of network bandwidth while scanning computers
Answer: (SHOW ANSWER)

NEW QUESTION: 280
If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this result?

A. Accurate identification
B. Unsuccessful identification
C. Suspected tampering
D. User error
Answer: (SHOW ANSWER)

NEW QUESTION: 281

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. Threat modelling
B. Source code review
C. Automated testing
D. Acceptance testing
Answer: (SHOW ANSWER)

NEW QUESTION: 282
An application team is running tests to ensure that user entry fields will not accept invalid input of any length. What type of negative testing is this an example of?

A. Reasonable data
B. Population of required fields
C. Allowed number of characters
D. Session testing
Answer: (SHOW ANSWER)
Reference: https://www.softwaretestinghelp.com/what-is-negative-testing/

NEW QUESTION: 283
Which of the following entails identification of data end links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

A. Security portfolio management
B. Risk assessment
C. Risk management
D. Security governance
Answer: (SHOW ANSWER)

NEW QUESTION: 284
What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

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

NEW QUESTION: 285
Which of the following would an attacker be able to accomplish through the use of Remote Access Tools (RAT)?

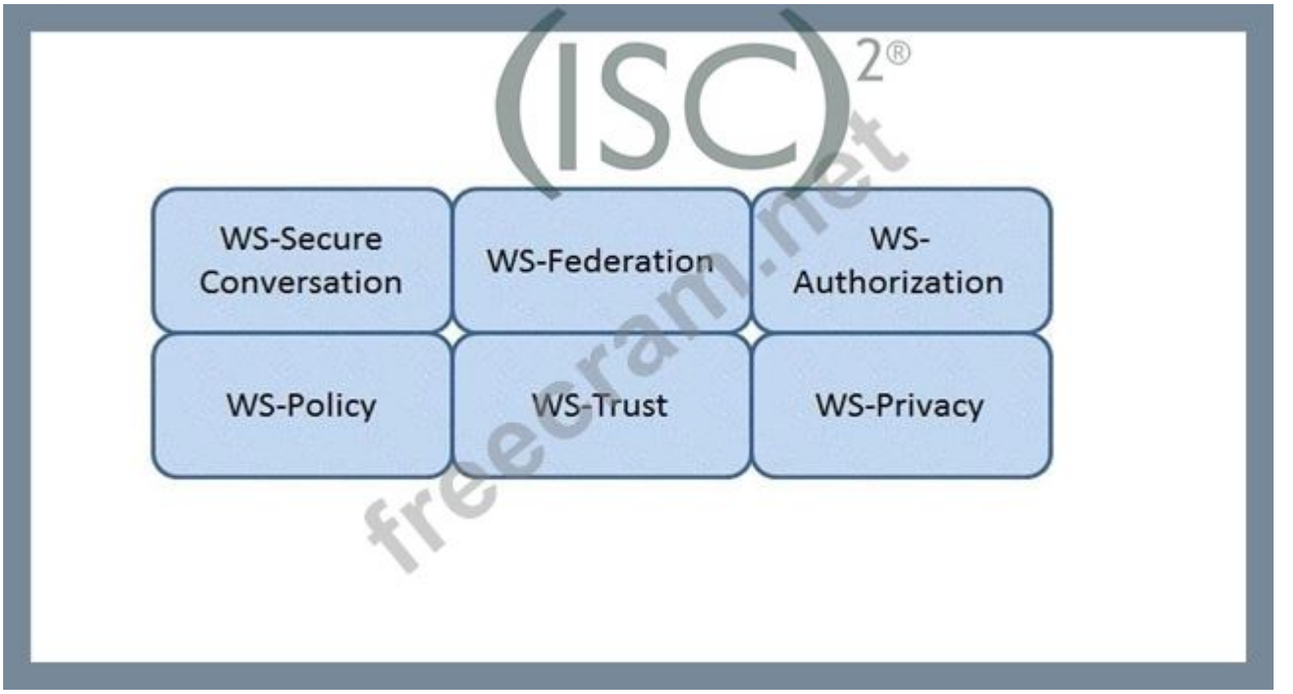
A. Reduce the probability of identification
B. Detect further compromise of the target
C. Destabilize the operation of the host
D. Maintain and expand control
Answer: (SHOW ANSWER)

NEW QUESTION: 286
Which of the following is TRUE about Disaster Recovery Plan (DRP) testing?
A. The company is fully prepared for a disaster if all tests pass.
B. Testing should not be done until the entire disaster plan can be tested.
C. Testing should continue even if components of the test fail.
D. Operational networks are usually shut down during testing.
Answer: (SHOW ANSWER)

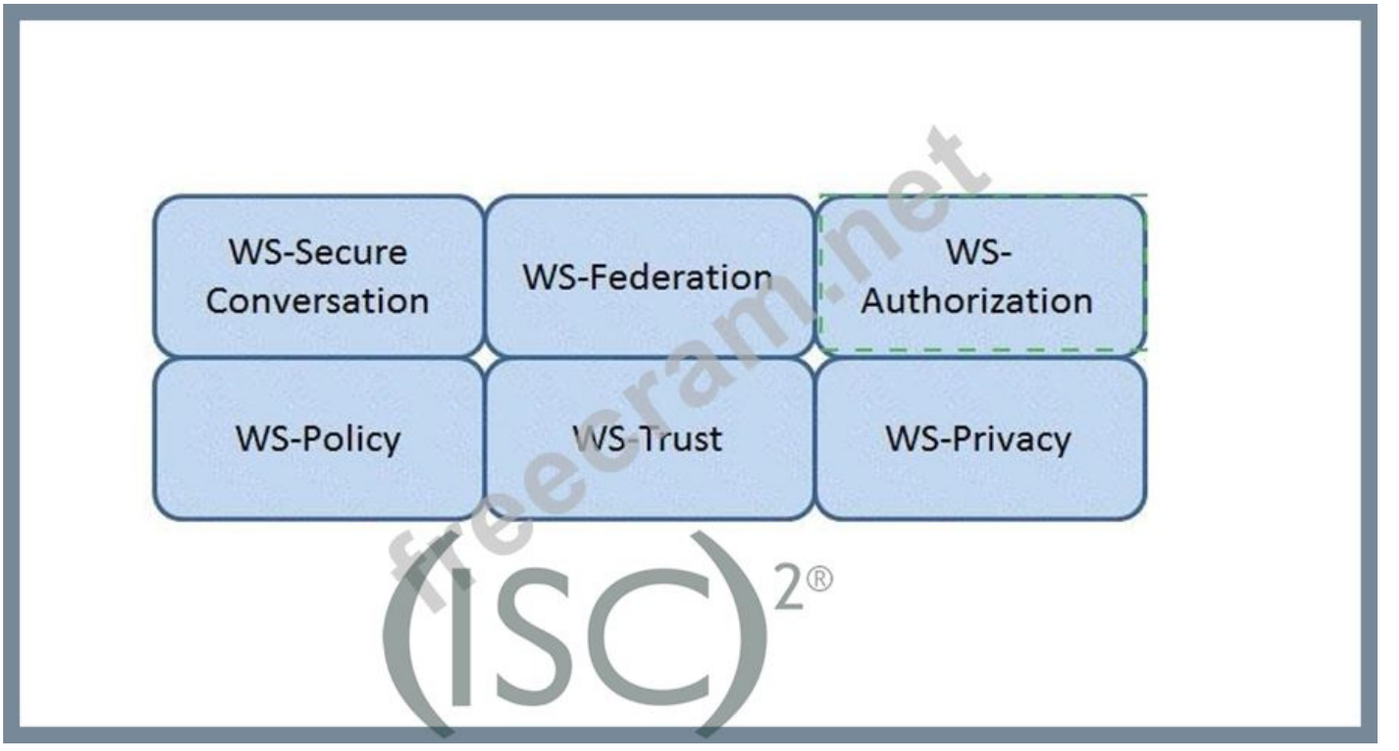
NEW QUESTION: 287
With what frequency should monitoring of a control occur when implementing information security continuous monitoring (ISCM) solutions?
A. At a rate concurrent with the volatility of the security control
B. Before and after each change of the control
C. Continuously without exception for all security controls
D. Only during system implementation and decommissioning
Answer: (SHOW ANSWER)

NEW QUESTION: 288
Which of the following is the MOST effective method of mitigating data theft from an active user workstation?
A. Disable use of portable devices
B. Implement full-disk encryption
C. Enable multifactor authentication
D. Deploy file integrity checkers
Answer: (SHOW ANSWER)

NEW QUESTION: 289
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.



Answer:



Explanation
WS-Authorization
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION: 290
Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

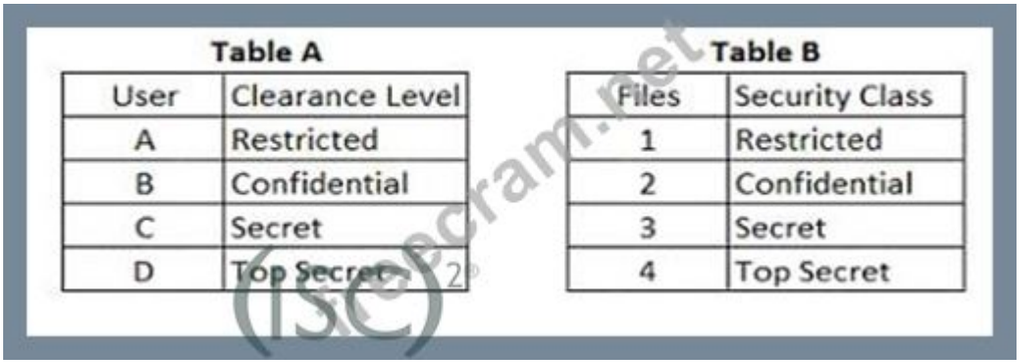


Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

Which of the following is true according to the star property (*property)?

A. User A can write to File 1

B. User C can write to File 1

C. User D can write to File 1

D. User B can write to File 1

Answer: A (LEAVE A REPLY)

NEW QUESTION: 291

A development operations team would like to start building new applications delegating the cybersecurity responsibility as much as possible to the service provider. Which of the following environments BEST fits their need?

A. Self-hosted Virtual Machine (VM)

B. On premises Virtual Machine (VM)

C. Cloud application container within a Virtual Machine (VM)

D. Cloud Virtual Machines (VM)

Answer: (SHOW ANSWER)

NEW QUESTION: 292

Which of the following is a recommended alternative to an integrated email encryption system?

A. Encrypt sensitive data separately in attachments

B. Store sensitive information to be sent in encrypted drives

C. Send sensitive data in separate emails

D. Sign emails containing sensitive data

Answer: (SHOW ANSWER)

NEW QUESTION: 293

What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

A. Plan of Action and Milestones {POA&M)

B. Security Assessment Report (SAR)

C. Business Impact Analysis (BIA)

D. Security Assessment Plan (SAP)
Answer: (SHOW ANSWER)

NEW QUESTION: 294
The core component of Role Based Access Control (RBAC) must be constructed of defined data elements.
Which elements are required?
A. Users, permissions, operations, and protected objects
B. Roles, operations, accounts, and protected objects
C. Roles, accounts, permissions, and protected objects
D. Users, roles, operations, and protected objects
Answer: (SHOW ANSWER)

NEW QUESTION: 295
Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the
A. structured code review.
B. cost benefit analysis.
C. security impact analysis.
D. routine self assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 296
Discretionary Access Control (DAC) restricts access according to
A. page views within an application.
B. data classification labeling.
C. management accreditation.
D. authorizations granted to the user.
Answer: (SHOW ANSWER)

NEW QUESTION: 297
Which of the following MUST be done when promoting a security awareness program to senior management?
A. Explain how hackers have enhanced information security
B. Ensure that the security presentation is designed to be all-inclusive
C. Show the need for security; identify the message and the audience
D. Notify them that their compliance is mandatory
Answer: (SHOW ANSWER)

NEW QUESTION: 298
When should an application invoke re-authentication in addition to initial user authentication?

A. For each business process
B. Periodically during a session
C. After a period of inactivity
D. At the application sign-off
Answer: (SHOW ANSWER)

NEW QUESTION: 299
Due to system constraints, a group of system administrators must share a high-level access set of credentials.
Which of the following would be
A. Increased console lockout times for failed logon attempts
B. Reduce the group in size
C. A credential check-out process for a per-use basis
D. Full logging on affected systems
Answer: (SHOW ANSWER)
Explanation
Section: Security Operations

NEW QUESTION: 300
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?
A. Integrity and Availability
B. Confidentiality and Integrity
C. Availability and Accountability
D. Accountability and Assurance
Answer: (SHOW ANSWER)

NEW QUESTION: 301
When adopting software as a service (Saas), which security responsibility will remain with remain with the adopting organization?
A. Data classification
B. Physical security
C. Network control
D. Application layer control
Answer: (SHOW ANSWER)

NEW QUESTION: 302
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
When determining appropriate resource allocation, which of the following is MOST important to monitor?
A. Number of system compromises
B. Number of audit findings
C. Number of additional assets
D. Number of staff reductions
Answer: (SHOW ANSWER)

NEW QUESTION: 303
The use of proximity card to gain access to a building is an example of what type of security control?
A. Physical
B. Logical
C. Legal
D. Procedural
Answer: (SHOW ANSWER)

NEW QUESTION: 304
A security professional is asked to provide a solution that restricts a bank teller to only perform a savings deposit transaction but allows a supervisor to perform corrections after the transaction.
Which of the following is the MOST effective solution?
A. Access is based on rules.
B. Access is based on data sensitivity.
C. Access is based on user's role.
D. Access is determined by the system.
Answer: (SHOW ANSWER)

NEW QUESTION: 305
Additional padding may be added to toe Encapsulating Security Protocol (ESP) b trailer to provide which of the following?
A. Protection against replay attack

B. Access control
C. Partial traffic flow confidentiality
D. Data origin authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 306
How does identity as a service (IDaaS) provide an easy mechanism for integrating identity service into individual applications with minimal development effort?
A. By integrating internal provisioning procedures with external authentication processes
B. By keeping all user information in easily accessible cloud repositories
C. By allowing for internal provisioning of user accounts
D. By allowing the identification logic and storage of an identity s attributes to be maintained externally
Answer: (SHOW ANSWER)

NEW QUESTION: 307
The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the
A. ability to tailor security parameters based on location.
B. right to disguise the software's geographic origin.
C. right to refuse or permit commercial rentals.
D. ability to confirm license authenticity of their works.
Answer: (SHOW ANSWER)

NEW QUESTION: 308
Which of the following does Temporal Key Integrity Protocol (TKIP) support?
A. Wired Equivalent Privacy (WEP) systems
B. Synchronization of multiple devices
C. Coordination of IEEE 802.11 protocols
D. Multicast and broadcast messages
Answer: (SHOW ANSWER)

NEW QUESTION: 309
Why do certificate Authorities (CA) add value to the security of electronic commerce transactions?
A. They verify the transaction parties' private keys.
B. They maintain the private keys of transition parties.
C. They provide a secure communication enamel to the transaction parties.
D. They maintain the certificate revocation list.
Answer: (SHOW ANSWER)

NEW QUESTION: 310

Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
What MUST the plan include in order to reduce client-side exploitation?

A. Proxy configuration
B. Network firewall procedures
C. Employee education
D. Approved web browsers
Answer: (SHOW ANSWER)

NEW QUESTION: 311
When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include
A. adequate distance from and lack of access to adjacent buildings.
B. hardened building construction with consideration of seismic factors.
C. proximity to high crime areas of the city.
D. curved roads approaching the data center.
Answer: (SHOW ANSWER)

NEW QUESTION: 312
Which of the following mandates the amount and complexity of security controls applied to a security risk?
A. Risk mitigation
B. Security vulnerabilities
C. Security staff
D. Risk tolerance
Answer: A (LEAVE A REPLY)