ISC.CISSP.v2017-11-26.q373

Exam Code:	CISSP
Exam Name:	Certified Information Systems Security Professional (CISSP)
Certification Provider:	ISC
Free Question Number:	373
Version:	v2017-11-26
# of views:	3411
# of Questions views:	293084
https://www.freecram.net/torrent/ISC.CISSP.v2017-11-26.q373.html	

NEW QUESTION: 1
With data labeling, which of the following MUST be the key decision maker?
A. Information security
B. Departmental management
C. Data owner
D. Data custodian
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following is a critical factor for implementing a successful data classification program?
A. Information security sponsorship
B. Executive sponsorship
C. End-user acceptance
D. Internal audit acceptance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
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. Unsuccessful identification
B. Accurate identification
C. User error
D. Suspected tampering
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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.
What MUST the access control logs contain in addition to the identifier?
A. Denied access attempts
B. Time of the access
C. Security classification
D. Associated clearance
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?
A. Proximity to an airline flight path
B. Vulnerability to natural disasters
C. Vulnerability to crime
D. Adjacent buildings and businesses
Answer: (SHOW ANSWER)

NEW QUESTION: 6
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 additional assets
B. Number of staff reductions
C. Number of audit findings
D. Number of system compromises
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which type of control recognizes that a transaction amount is excessive in accordance with
corporate policy?
A. Investigation
B. Prevention
C. Detection
D. Correction
Answer: (SHOW ANSWER)

NEW QUESTION: 8

If an attacker in a SYN flood attack uses someone else's valid host address as the source address, the system under attack will send a large number of Synchronize/Acknowledge (SYN/ACK) packets to the

A. default gateway.

B. local interface being attacked.

C. specified source address.

D. attacker's address.

Answer: (SHOW ANSWER)

NEW QUESTION: 9

The goal of software assurance in application development is to

A. encourage the development of open source applications.

B. facilitate the creation of Trusted Computing Base (TCB) systems.

C. enable the development of High Availability (HA) systems.

D. prevent the creation of vulnerable applications.

Answer: (SHOW ANSWER)

NEW QUESTION: 10

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

A. Cross Origin Resource Sharing (CORS)

B. Web Interface Definition Language (IDL)

C. WebSockets

D. Document Object Model (DOM) trees

Answer: (SHOW ANSWER)

NEW QUESTION: 11

DRAG DROP

Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

Secure Architecture	Do you advertise shared security services with guidance for project teams?
Education & Guidance	Are most people tested to ensure a baseline skill- set for secure development practices?
Strategy & Metrics	Does most of the organization know about what's required based on risk ratings?
Vulnerability Management	Are most project teams aware of their security point(s) of contact and response team(s)?

Answer:

NEW QUESTION: 12
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: 13
An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?
A. Servers are able to issue digital certificates to the client.
B. Servers can authenticate themselves to the client.
C. Mutual authentication is available between the clients and servers.
D. Clients can authenticate themselves to the servers.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
What is the BEST method to detect the most common improper initialization problems in programming languages?
A. Perform input validation on any numeric inputs by assuring that they are within the expected range.
B. Use and specify a strong character encoding.
C. Use automated static analysis tools that target this type of weakness.
D. Use data flow analysis to minimize the number of false positives.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
What is an effective practice when returning electronic storage media to third parties for repair?
A. Physically breaking parts of the media that may contain sensitive data.

B. Establishing a contract with the third party regarding the secure handling of the media.
C. Disassembling the media and removing parts that may contain sensitive data.
D. Ensuring the media is not labeled in any way that indicates the organization's name.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
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 security program can be considered effective when
A. audits are regularly performed and reviewed.
B. risk is lowered to an acceptable level.
C. backups are regularly performed and validated.
D. vulnerabilities are proactively identified.
Answer: (SHOW ANSWER)

NEW QUESTION: 17
The PRIMARY purpose of a security awareness program is to
A. ensure that everyone understands the organization's policies and procedures.
B. communicate that access to information will be granted on a need-to-know basis.
C. comply with regulations related to data and information protection.
D. warn all users that access to all systems will be monitored on a daily basis.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
What security management control is MOST often broken by collusion?
A. Separation of duties
B. Least privilege model
C. Job rotation
D. Increased monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which of the following analyses is performed to protect information assets?
A. Feasibility analysis

B. Data analysis
C. Business impact analysis
D. Cost benefit analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following is the MOST crucial for a successful audit plan?
A. Acquiring evidence of systems that are not compliant
B. Defining the scope of the audit to be performed
C. Identifying the security controls to be implemented
D. Working with the system owner on new controls
Answer: (SHOW ANSWER)

NEW QUESTION: 21
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: 22
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 picking
B. Lock pinging
C. Lock bricking
D. Lock bumping
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which of the following is an attacker MOST likely to target to gain privileged access to a system?
A. Log files containing system calls
B. Programs that write to user directories
C. Log files containing sensitive information
D. Programs that write to system resources
Answer: (SHOW ANSWER)

NEW QUESTION: 24

Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?
A. It has normalized severity ratings.
B. It requires a robust risk management framework to be put in place.
C. It has many worksheets and practices to implement.
D. It aims to calculate the risk of published vulnerabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which of the following describes the BEST configuration management practice?
A. After installing a new system, the configuration files are copied to a separate back-up system and hashed to detect tampering.
B. After installing a new system, the configuration files are copied to an air-gapped system and hashed to detect tampering.
C. The firewall rules are backed up to an air-gapped system.
D. A baseline configuration is created and maintained for all relevant systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
A Simple Power Analysis (SPA) attack against a device directly observes which of the following?
A. Magnetism
B. Consumption
C. Static discharge
D. Generation
Answer: (SHOW ANSWER)

NEW QUESTION: 27
What is the MAIN feature that onion routing networks offer?
A. Anonymity
B. Resilience
C. Traceability
D. Non-repudiation
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Secure Sockets Layer (SSL) encryption protects
A. data at rest.
B. data availability.
C. the source IP address.
D. data transmitted.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Retaining system logs for six months or longer can be valuable for what activities?

A. Disaster recovery and business continuity
B. Physical and logical access control
C. Forensics and incident response
D. Identity and authorization management
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which of the following PRIMARILY contributes to security incidents in web-based applications?
A. System incompatibility and patch management
B. Systems administration and operating systems
C. Third-party applications and change controls
D. Improper stress testing and application interfaces
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which one of the following is a fundamental objective in handling an incident?
A. To prosecute the attacker
B. To perform full backups of the system
C. To restore control of the affected systems
D. To confiscate the suspect's computers
Answer: (SHOW ANSWER)

NEW QUESTION: 32
What does secure authentication with logging provide?
A. Access accountability
B. Data integrity
C. Encryption logging format
D. Segregation of duties
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

A. Degausser products may not be properly maintained and operated.
B. Commercial products often have serious weaknesses of the magnetic force available in the degausser product.
C. The inability to turn the drive around in the chamber for the second pass due to human error.
D. Inadequate record keeping when sanitizing media.
Answer: (SHOW ANSWER)

NEW QUESTION: 34
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?
A. Integrity
B. Confidentiality
C. Availability
D. Ownership
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which of the following are required components for implementing software configuration management systems?
A. Audit control and signoff
B. Rollback and recovery processes
C. Regression testing and evaluation
D. User training and acceptance
Answer: (SHOW ANSWER)

NEW QUESTION: 36
What is one way to mitigate the risk of security flaws in custom software?
A. Purchase only Commercial Off-The-Shelf (COTS) products
B. Include security language in the Earned Value Management (EVM) contract
C. Include security assurance clauses in the Service Level Agreement (SLA)
D. Purchase only software with no open source Application Programming Interfaces (APIs)
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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. Lack of Data Loss Prevention (DLP) tools
D. Ineffective data classification
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?
A. Re-image the computer
B. Find and remove all installation files
C. Run software uninstall
D. Delete all cookies stored in the web browser cache
Answer: (SHOW ANSWER)

NEW QUESTION: 39
The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide
A. data integrity.
B. defense in depth.
C. data availability.
D. non-repudiation.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
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. opportunity to sniff network traffic exists.
C. storage devices are protected against availability attacks.
D. confidentiality of the traffic is protected.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?
A. immature security controls and procedures
B. unanticipated increases in security incidents and threats
C. poor governance over security processes and procedures
D. variances against regulatory requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which of the following is the MAIN goal of a data retention policy?
A. Ensure the integrity and availability of data for a predetermined amount of time.
B. Ensure that data recovery can be done on the data.
C. Ensure the integrity and confidentiality of data for a predetermined amount of time.

D. Ensure that data is destroyed properly.
Answer: (SHOW ANSWER)

NEW QUESTION: 43
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. right to disguise the software's geographic origin.
B. ability to tailor security parameters based on location.
C. ability to confirm license authenticity of their works.
D. right to refuse or permit commercial rentals.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Which of the following MOST influences the design of the organization's electronic monitoring policies?
A. Results of background checks
B. Workplace privacy laws
C. Level of organizational trust
D. Business ethical considerations
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Discretionary Access Control (DAC) is based on which of the following?
A. Security labels and privileges
B. Identification of subjects and objects
C. Standards and guidelines
D. Information source and destination
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which one of the following considerations has the LEAST impact when considering transmission security?
A. Network availability
B. Data integrity
C. Node locations
D. Network bandwidth
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which of the following is considered best practice for preventing e-mail spoofing?
A. Uniform Resource Locator (URL) filtering
B. Cryptographic signature
C. Reverse Domain Name Service (DNS) lookup
D. Spam filtering
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which one of the following is the MOST important in designing a biometric access system if it is essential that no one other than authorized individuals are admitted?
A. False Acceptance Rate (FAR)
B. Crossover Error Rate (CER)
C. False Rejection Rate (FRR)
D. Rejection Error Rate
Answer: (SHOW ANSWER)

NEW QUESTION: 49
The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using
A. GRANT and REVOKE.
B. ROLLBACK and TERMINATE.
C. INSERT and DELETE.
D. PUBLIC and PRIVATE.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
The goal of a Business Continuity Plan (BCP) training and awareness program is to
A. provide each recovery team with checklists and procedures.
B. describe the recovery organization to new employees.
C. enhance the skills required to create, maintain, and execute the plan.
D. provide for a high level of recovery in case of disaster.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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

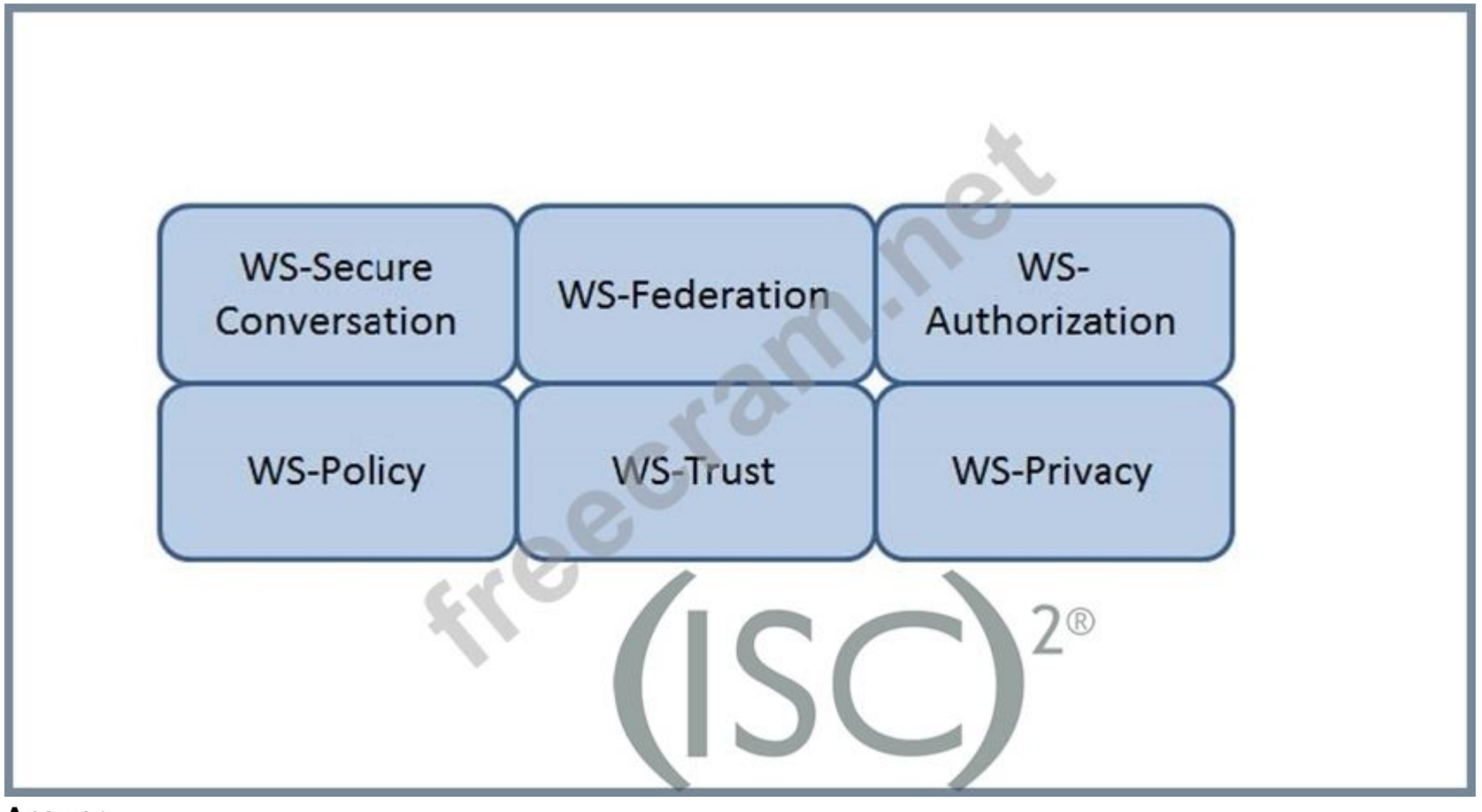
B. Organizational procedures designed to protect privacy information
C. Privacy-related regulations enforced by governing bodies applicable to the organization
D. Privacy best practices published by recognized security standards organizations
Answer: (SHOW ANSWER)

NEW QUESTION: 52
How does an organization verify that an information system's current hardware and software match the standard system configuration?
A. By running vulnerability scanning tools on all devices in the environment
B. By verifying all the approved security patches are implemented
C. By reviewing the configuration after the system goes into production
D. By comparing the actual configuration of the system against the baseline
Answer: (SHOW ANSWER)

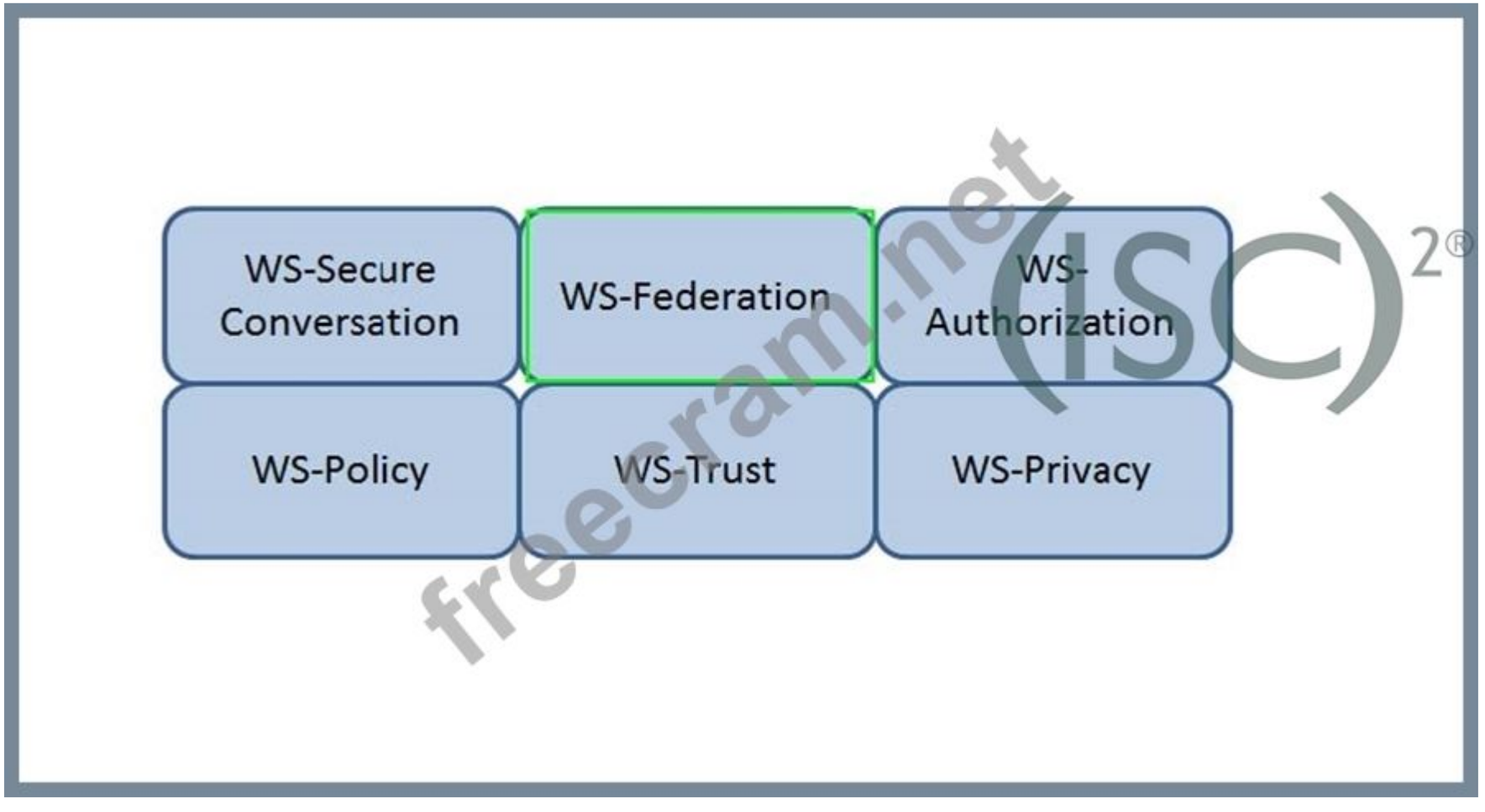
NEW QUESTION: 53
Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?
A. Secure card reader
B. Intrusion Prevention System (IPS)
C. Radio Frequency (RF) scanner
D. Anti-tampering
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which of the following violates identity and access management best practices?
A. System accounts
B. Privileged accounts
C. Generic accounts
D. User accounts
Answer: (SHOW ANSWER)

NEW QUESTION: 55
HOTSPOT
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.


WS-Secure Conversation
WS-Federation
WS-Authorization
WS-Policy
WS-Trust
WS-Privacy

Answer:


WS-Secure Conversation
WS-Federation
WS-Authorization
WS-Policy
WS-Trust
WS-Privacy

NEW QUESTION: 56
Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?
A. The radio spectrum is divided with multiple frequency carriers.
B. It uses a Subscriber Identity Module (SIM) for authentication.
C. The signal is difficult to read as it provides end-to-end encryption.
D. It uses encrypting techniques for all communications.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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: 58
A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?
A. Collector Accountability
B. Individual Participation
C. Collection Limitation
D. Onward transfer
Answer: (SHOW ANSWER)

NEW QUESTION: 59
What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?
A. Induction
B. Heuristic
C. Inference
D. Signature
Answer: (SHOW ANSWER)

NEW QUESTION: 60
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

A. Asymmetric encryption and User ID
B. Public Key Infrastructure (PKI) and digital signatures
C. Trusted server certificates and passphrases
D. User ID and password
Answer: (SHOW ANSWER)

NEW QUESTION: 61
An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the BEST response to the auditor?
A. Analyze the encrypted passwords for the auditor and show them the results.
B. Provide the encrypted passwords and analysis tools to the auditor for analysis.
C. Demonstrate that non-compliant passwords cannot be encrypted in the system.
D. Demonstrate that non-compliant passwords cannot be created in the system.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
DRAG DROP
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:

Security Engineering		Definition
Security Risk Treatment	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.**
Threat Assessment	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.**
Protection Needs	Threat Assessment	The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk	Security Risk Treatment	The method used to identify feasible security **risk mitigation options and plans.**

NEW QUESTION: 63

What is the GREATEST challenge to identifying data leaks?

A. Available technical tools that enable user activity monitoring.

B. Law enforcement participation to apprehend and interrogate suspects.

C. Documented asset classification policy and clear labeling of assets.

D. Senior management cooperation in investigating suspicious behavior.

Answer: (SHOW ANSWER)

NEW QUESTION: 64
What is the MOST important reason to configure unique user IDs?
A. Preventing password compromise
B. Reducing authentication errors
C. Supporting Single Sign On (SSO)
D. Supporting accountability
Answer: (SHOW ANSWER)

NEW QUESTION: 65
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. Deploy file integrity checkers
D. Enable multifactor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following is generally indicative of a replay attack when dealing with biometric authentication?
A. False Acceptance Rate (FAR) is greater than 1 in 100,000
B. Inadequately specified templates
C. Exact match
D. False Rejection Rate (FRR) is greater than 5 in 100
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?
A. Access based on user's role
B. Access based on data sensitivity
C. Access based on rules
D. Access determined by the system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
Which of the following is ensured when hashing files during chain of custody handling?
A. Availability
B. Integrity
C. Accountability
D. Non-repudiation
Answer: (SHOW ANSWER)

NEW QUESTION: 69
The Hardware Abstraction Layer (HAL) is implemented in the
A. application software.
B. network hardware.
C. system hardware.
D. system software.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
What security risk does the role-based access approach mitigate MOST effectively?
A. Inappropriate access requests
B. Segregation of duties conflicts within business applications
C. Excessive access rights to systems and data
D. Lack of system administrator activity monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 71
What should be the INITIAL response to Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts?
A. Disable or disconnect suspected target and source systems.
B. Verify the threat and determine the scope of the attack.
C. Ensure that the Incident Response Plan is available and current.
D. Determine the traffic's initial source and block the appropriate port.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?
A. Integration with organizational directory services for authentication
B. Identification of data location
C. Tokenization of data
D. Accommodation of hybrid deployment models
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following is the MOST effective attack against cryptographic hardware modules?
A. Plaintext
B. Power analysis
C. Man-in-the-middle (MITM)
D. Brute force
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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. In the core of the building
B. In an exterior room with windows
C. On the top floor
D. In the basement
Answer: (SHOW ANSWER)

NEW QUESTION: 75
The use of proximity card to gain access to a building is an example of what type of security control?
A. Physical
B. Procedural
C. Legal
D. Logical
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?
A. Configuration Management
B. Data at rest encryption
C. Integrity checking software
D. Cyclic redundancy check (CRC)
Answer: (SHOW ANSWER)

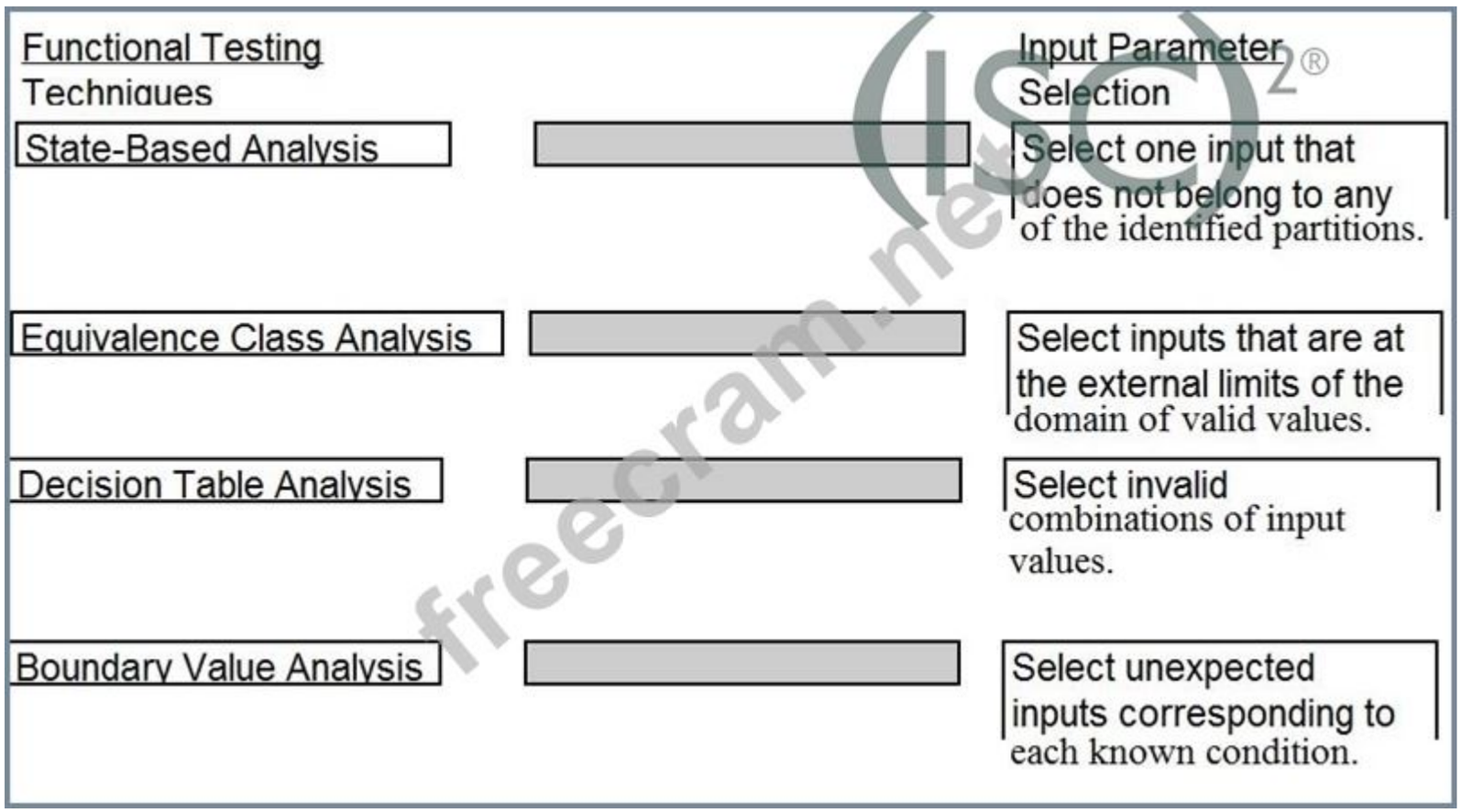
NEW QUESTION: 77
The BEST way to check for good security programming practices, as well as auditing for possible backdoors, is to conduct
A. impact assessments.
B. static analysis.
C. code reviews.
D. log auditing.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which of the following secures web transactions at the Transport Layer?
A. Secure Shell (SSH)
B. Socket Security (SOCKS)
C. Secure Sockets Layer (SSL)
D. Secure HyperText Transfer Protocol (S-HTTP)
Answer: (SHOW ANSWER)

NEW QUESTION: 79
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: 80
In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?
A. A functional evacuation of personnel
B. An activation of the backup site
C. A full-scale simulation of an emergency and the subsequent response functions
D. A specific test by response teams of individual emergency response functions
Answer: (SHOW ANSWER)

NEW QUESTION: 81
DRAG DROP
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.

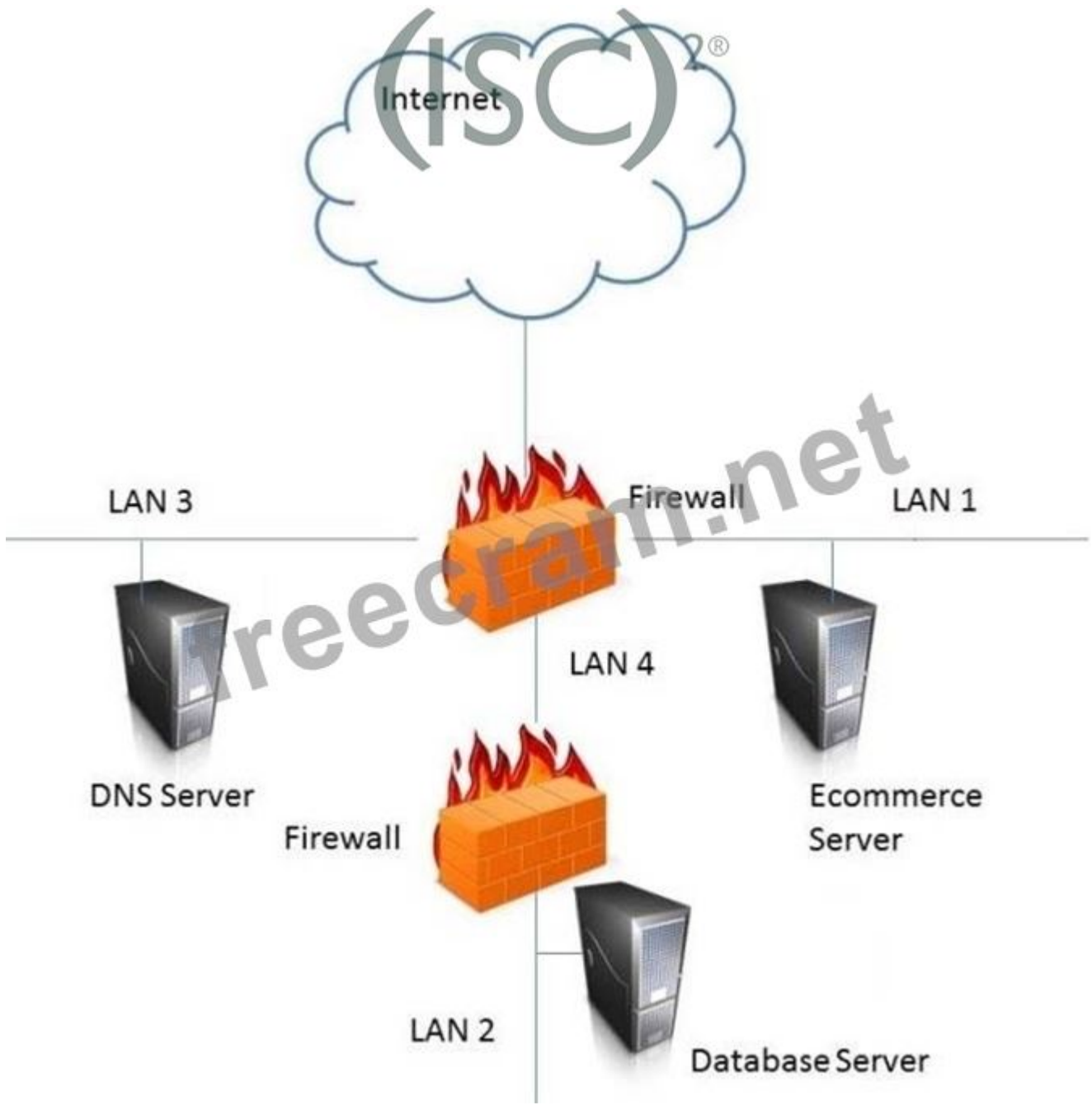

Functional Testing Techniques
Input Parameter Selection
State-Based Analysis
Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis
Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis
Select invalid combinations of input values.
Boundary Value Analysis
Select unexpected inputs corresponding to each known condition.

Answer:

Functional Testing Techniques		Input Parameter Selection
State-Based Analysis	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis	Decision Table Analysis	Select invalid combinations of input values.
Boundary Value Analysis	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

NEW QUESTION: 82
Which of the following can BEST prevent security flaws occurring in outsourced software development?
A. Delivery dates, change management control and budgetary control
B. Contractual requirements for code quality
C. Licensing, code ownership and intellectual property rights
D. Certification of the quality and accuracy of the work done
Answer: (SHOW ANSWER)

NEW QUESTION: 83
HOTSPOT
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:

NEW QUESTION: 84
What is the MOST effective method for gaining unauthorized access to a file protected with a long complex password?
A. Frequency analysis
B. Brute force attack
C. Social engineering
D. Dictionary attack
Answer: (SHOW ANSWER)

NEW QUESTION: 85

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

NEW QUESTION: 86
The BEST method of demonstrating a company's security level to potential customers is
A. a report from an external auditor.
B. responding to a customer's security questionnaire.
C. a site visit by a customer's security team.
D. a formal report from an internal auditor.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?
A. Information Systems Security Officer
B. System Security Architect
C. Security Requirements Analyst
D. Data Owner
Answer: (SHOW ANSWER)

NEW QUESTION: 88
According to best practice, which of the following is required when implementing third party software in a production environment?
A. Scan the application for vulnerabilities
B. Contract the vendor for patching
C. Negotiate end user application training
D. Escrow a copy of the software
Answer: (SHOW ANSWER)

NEW QUESTION: 89
What type of encryption is used to protect sensitive data in transit over a network?
A. Authentication Headers (AH)
B. Payload encryption and transport encryption
C. Point-to-Point Encryption (P2PE)
D. Keyed-Hashing for Message Authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 90

What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

A. Availability of the network connection
B. Regularly scheduled maintenance process
C. Physical access to the electronic hardware
D. Processing delays
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?
A. Parallel
B. Full interruption
C. Simulation
D. Read-through
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?
A. It is characterized by the stateless behavior of a process implemented in a function.
B. Test inputs are obtained from the derived boundaries of the given functional specifications.
C. An entire partition can be covered by considering only one representative value from that partition.
D. It is useful for testing communications protocols and graphical user interfaces.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.
As part of the authentication process, which of the following must the end user provide?
A. An access token
B. A password
C. A username
D. A username and password
Answer: (SHOW ANSWER)

NEW QUESTION: 94

Which of the following is the PRIMARY concern when using an Internet browser to access a cloud-based service?
A. Insecure implementation of Application Programming Interfaces (API)
B. Improper use and storage of management keys
C. Vulnerabilities within protocols that can expose confidential data
D. Misconfiguration of infrastructure allowing for unauthorized access
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following is the MOST difficult to enforce when using cloud computing?
A. Data backup
B. Data disposal
C. Data access
D. Data recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Who is ultimately responsible to ensure that information assets are categorized and adequate measures are taken to protect them?
A. Data/Information/Business Owners
B. Executive Management
C. Chief Information Security Officer
D. Data Custodian
Answer: (SHOW ANSWER)

NEW QUESTION: 97
A network scan found 50% of the systems with one or more critical vulnerabilities. Which of the following represents the BEST action?
A. Assess vulnerability risk and program effectiveness.
B. Assess vulnerability risk and business impact.
C. Disconnect all systems with critical vulnerabilities.
D. Disconnect systems with the most number of vulnerabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?
A. Dynamic separation of duties
B. The Bell-LaPadula security model
C. Hierarchical inheritance
D. The Clark-Wilson security model
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following documents explains the proper use of the organization's assets?
A. Acceptable use policy
B. Access control policy
C. Human resources policy
D. Code of ethics
Answer: (SHOW ANSWER)

NEW QUESTION: 100
Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

A. Smurf
B. Denial of Service (DoS)
C. Rootkit exploit
D. Cross site scripting (XSS)
Answer: (SHOW ANSWER)

NEW QUESTION: 101
The process of mutual authentication involves a computer system authenticating a user and authenticating the
A. user to the audit process.
B. user's access to all authorized objects.
C. computer system to the audit process.
D. computer system to the user.
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Which of the following is a security limitation of File Transfer Protocol (FTP)?
A. Anonymous access is allowed.
B. Passive FTP is not compatible with web browsers.
C. Authentication is not encrypted.
D. FTP uses Transmission Control Protocol (TCP) ports 20 and 21.
Answer: (SHOW ANSWER)

NEW QUESTION: 103
What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?
A. Conduct a risk assessment
B. Identify regulatory requirements
C. Review the security baseline configuration
D. Determine business drivers

Answer: (SHOW ANSWER)

NEW QUESTION: 104
The application of which of the following standards would BEST reduce the potential for data breaches?
A. ISO 26000
B. ISO 27001
C. ISO 20121
D. ISO 9000
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following defines the key exchange for Internet Protocol Security (IPSec)?
A. Secure Sockets Layer (SSL) key exchange
B. Security Key Exchange (SKE)
C. Internet Key Exchange (IKE)
D. Internet Control Message Protocol (ICMP)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 106
What is an important characteristic of Role Based Access Control (RBAC)?
A. Requires two factor authentication
B. Relies on rotation of duties
C. Supports Mandatory Access Control (MAC)
D. Simplifies the management of access rights
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Data remanence refers to which of the following?
A. The retention period required by law or regulation.
B. The remaining photons left in a fiber optic cable after a secure transmission.
C. The residual information left on magnetic storage media after a deletion or erasure.
D. The magnetic flux created when removing the network connection from a server or personal computer.
Answer: (SHOW ANSWER)

NEW QUESTION: 108

A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

A. it protects against unauthorized access.

B. the scalability of token enrollment.

C. it simplifies user access administration.

D. increased accountability of end users.

Answer: (SHOW ANSWER)

NEW QUESTION: 109

A Business Continuity Plan (BCP) is based on

A. a review of the business processes and procedures.

B. an existing BCP from a similar organization.

C. the policy and procedures manual.

D. a standard checklist of required items and objectives.

Answer: (SHOW ANSWER)

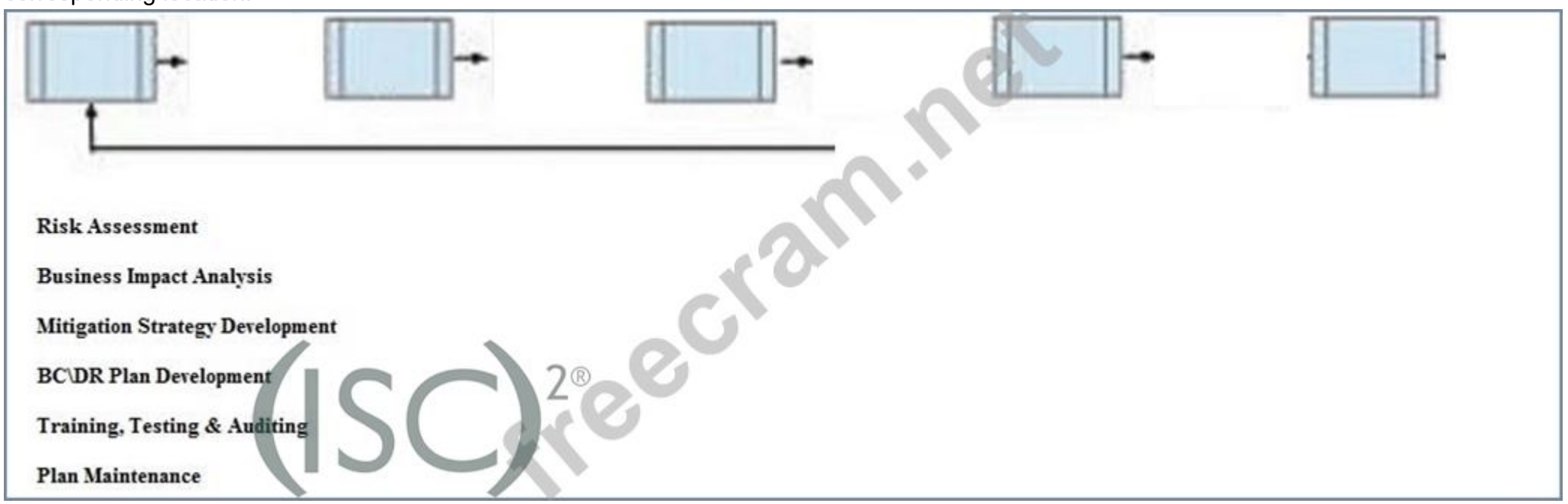
NEW QUESTION: 110

DRAG DROP

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?

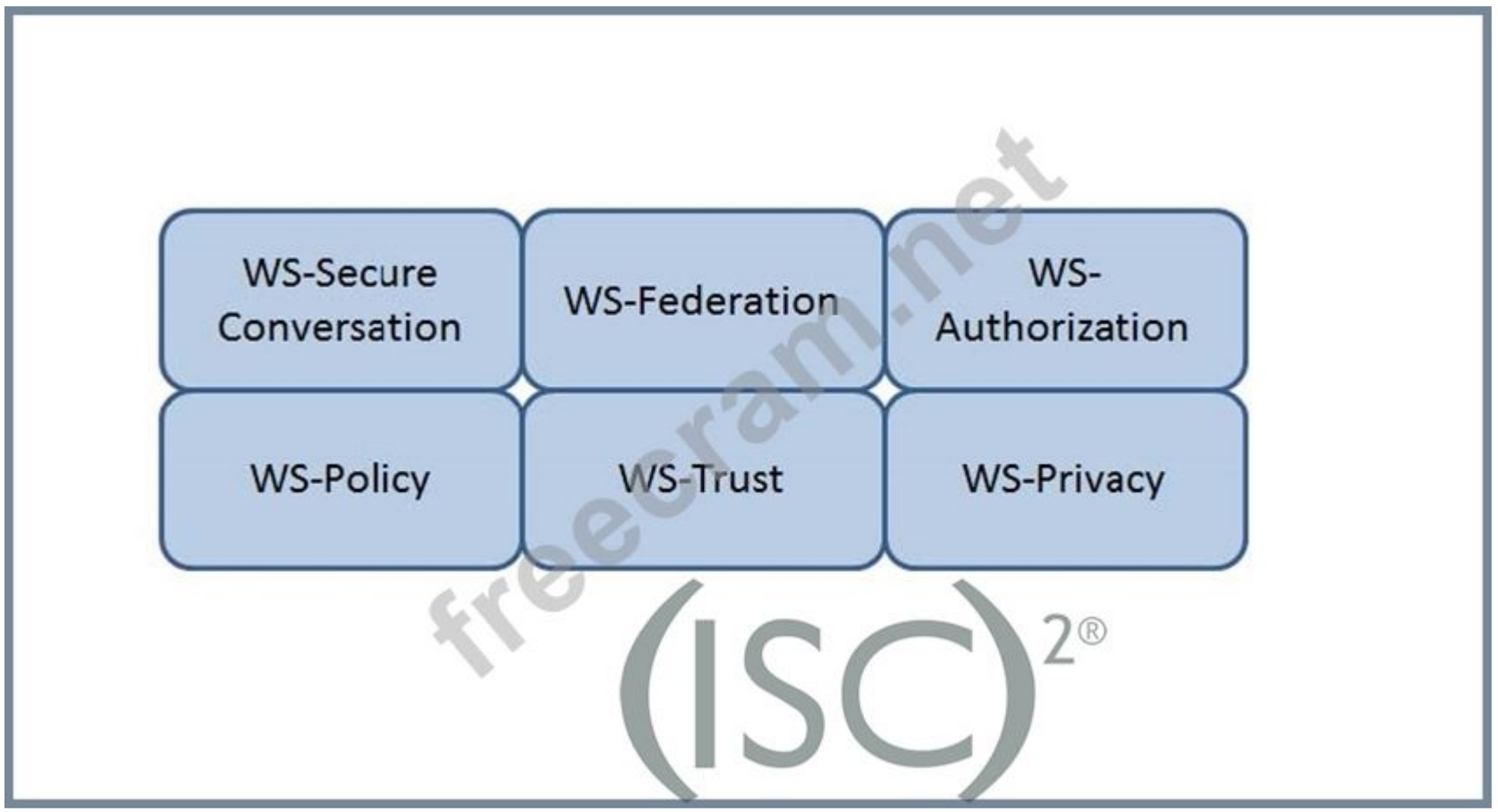
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.



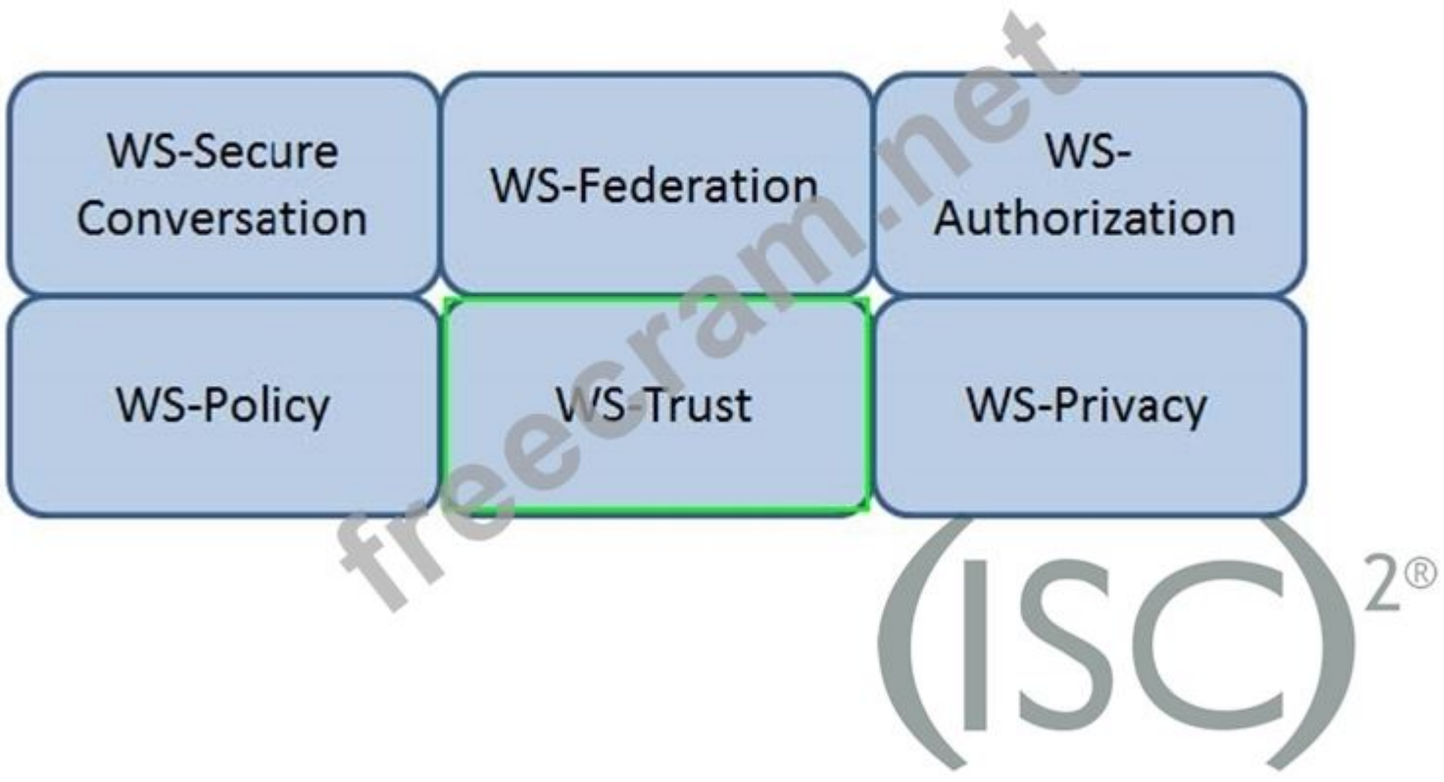
Answer:

NEW QUESTION: 111
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?
A. Anti-spyware software
B. Anti-virus software
C. Intrusion Prevention System (IPS)
D. Integrity checking software
Answer: (SHOW ANSWER)

NEW QUESTION: 112
HOTSPOT
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.


WS-Secure Conversation
WS-Federation
WS-Authorization
WS-Policy
WS-Trust
WS-Privacy

Answer:


WS-Secure Conversation
WS-Federation
WS-Authorization
WS-Policy
WS-Trust
WS-Privacy

NEW QUESTION: 113
From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?
A. Block all Transmission Control Protocol (TCP) connections.
B. Configure secondary servers to use the primary server as a zone forwarder.
C. Disable all recursive queries on the name servers.
D. Limit zone transfers to authorized devices.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 114
When designing a networked Information System (IS) where there will be several different types of individual access, what is the FIRST step that should be taken to ensure all access control requirements are addressed?
A. Develop a Role Based Access Control (RBAC) list.
B. Create a user access matrix.
C. Create a user profile.
D. Develop an Access Control List (ACL).
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following provides effective management assurance for a Wireless Local Area Network (WLAN)?
A. Setting the radio frequency to the minimum range required
B. Verifying that all default passwords have been changed
C. Maintaining an inventory of authorized Access Points (AP) and connecting devices
D. Establishing a Virtual Private Network (VPN) tunnel between the WLAN client device and a VPN concentrator
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?
A. Interface testing
B. Authentication validation
C. Periodic log reviews
D. Policy documentation review
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which of the following is TRUE about Disaster Recovery Plan (DRP) testing?
A. Testing should not be done until the entire disaster plan can be tested.
B. The company is fully prepared for a disaster if all tests pass.
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: 118
Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?
A. Review automated patch deployment reports
B. Automated vulnerability scanning
C. Periodic third party vulnerability assessment
D. Perform vulnerability scan by security team
Answer: (SHOW ANSWER)

NEW QUESTION: 119
A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as
A. rule based access controls.
B. separation of duties.
C. Mandatory Access Control (MAC).
D. least privilege.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
If compromised, which of the following would lead to the exploitation of multiple virtual machines?
A. Virtual device drivers
B. Virtual machine file system
C. Virtual machine monitor
D. Virtual machine instance
Answer: (SHOW ANSWER)

NEW QUESTION: 121
What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?
A. Some users are not provisioned into the service.
B. SAML tokens are provided by the on-premise identity provider.
C. SAML tokens contain user information.
D. Single users cannot be revoked from the service.
Answer: (SHOW ANSWER)

NEW QUESTION: 122

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

NEW QUESTION: 123
Without proper signal protection, embedded systems may be prone to which type of attack?
A. Denial of Service (DoS)
B. Information disclosure
C. Brute force
D. Tampering
Answer: (SHOW ANSWER)

NEW QUESTION: 124
The key benefits of a signed and encrypted e-mail include
A. confidentiality, non-repudiation, and authentication.
B. confidentiality, authentication, and authorization.
C. non-repudiation, confidentiality, and authorization.
D. non-repudiation, authorization, and authentication.
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?
A. Acoustic cryptanalysis
B. Side channel
C. Timing
D. Cold boot
Answer: (SHOW ANSWER)

NEW QUESTION: 126
Which of the following methods provides the MOST protection for user credentials?
A. Forms-based authentication
B. Basic authentication
C. Self-registration
D. Digest authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 127
The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

A. A metadirectory
B. Single Sign-On (SSO)
C. Two-factor authentication
D. User self-service
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?
A. Data-Link Layer
B. Network Layer
C. Application Layer
D. Physical Layer
Answer: (SHOW ANSWER)

NEW QUESTION: 129
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted
A. bi-annually.
B. quarterly.
C. annually.
D. monthly.
Answer: (SHOW ANSWER)

NEW QUESTION: 130
After acquiring the latest security updates, what must be done before deploying to production systems?
A. Install the patches on a test system
B. Assess the severity of the situation
C. Subscribe to notifications for vulnerabilities
D. Use tools to detect missing system patches
Answer: (SHOW ANSWER)

NEW QUESTION: 131
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?
A. Build a baseline of normal or safe system events for review
B. Automatically whitelist actions or files known to the system
C. Determine which files are unsafe to access and blacklist them
D. Automatically create exceptions for specific actions or files
Answer: (SHOW ANSWER)

NEW QUESTION: 132
Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

A. Application hardening
B. Role Based Access Control (RBAC)
C. Federated Identity Management (IdM)
D. Biometric access control
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Which one of the following affects the classification of data?
A. Minimum query size
B. Multilevel Security (MLS) architecture
C. Passage of time
D. Assigned security label
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which of the following is the BEST approach to take in order to effectively incorporate the concepts of business continuity into the organization?
A. Develop training and awareness programs that involve all stakeholders
B. Ensure plans do not violate the organization's cultural objectives and goals
C. Ensure end users are aware of the planning activities
D. Validate all regulatory requirements are known and fully documented
Answer: (SHOW ANSWER)

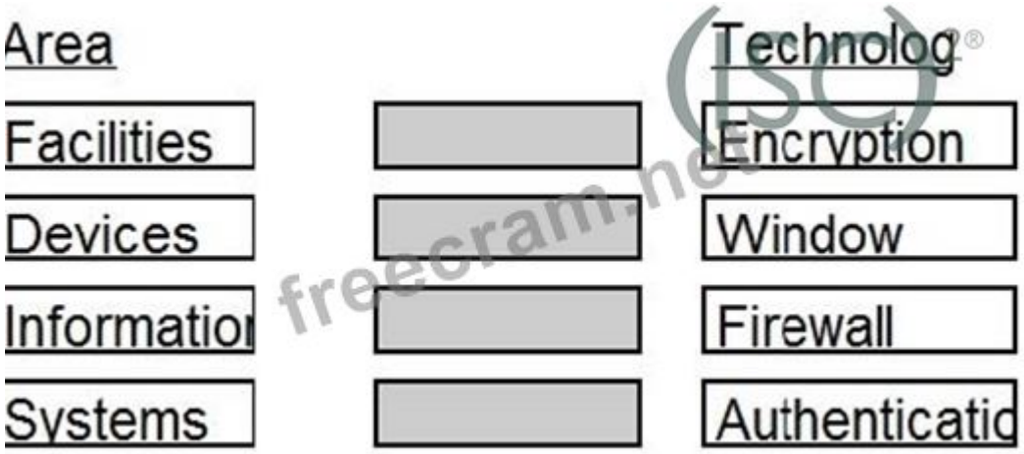
NEW QUESTION: 135
Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?
A. End-to-end data encryption for data in transit
B. Limited collection of individuals' confidential data
C. A strong breach notification process
D. Continuous monitoring of potential vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?
A. It is characterized by the stateless behavior of a process implemented in a function.
B. It is useful for testing communications protocols and graphical user interfaces.
C. An entire partition can be covered by considering only one representative value from that partition.
D. Test inputs are obtained from the derived threshold of the given functional specifications.
Answer: (SHOW ANSWER)

NEW QUESTION: 137
A disadvantage of an application filtering firewall is that it can lead to
A. performance degradation due to the rules applied.
B. Internet Protocol (IP) spoofing by hackers.
C. loss of packets on the network due to insufficient bandwidth.
D. a crash of the network as a result of user activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?
A. Use of a unified messaging.
B. Use of Network Access Control (NAC) on switches.
C. Use of Request for Comments (RFC) 1918 addressing.
D. Use of separation for the voice network.
Answer: (SHOW ANSWER)

NEW QUESTION: 139
DRAG DROP
Given the various means to protect physical and logical assets, match the access management area to the technology.



Answer:

NEW QUESTION: 140

Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

A. Address Masking

B. Routing Information Protocol (RIP) Version 2

C. Application Proxy

D. Network Address Translation (NAT)

Answer: (SHOW ANSWER)

NEW QUESTION: 141

The three PRIMARY requirements for a penetration test are

A. A stated objective, liability waiver, and disclosed methodology

B. A general objective, unlimited time, and approval of the network administrator

C. An objective statement, disclosed methodology, and fixed cost

D. A defined goal, limited time period, and approval of management

Answer: (SHOW ANSWER)

NEW QUESTION: 142

Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

A. Hardware based encryption on dedicated physical servers.

B. Strong encryption and deletion of the virtual host after data is deleted.

C. Strong encryption and deletion of the keys after data is deleted.

D. Software based encryption with two factor authentication.

Answer: (SHOW ANSWER)

NEW QUESTION: 143

What is the PRIMARY reason for ethics awareness and related policy implementation?

A. It affects the workflow of an organization.

B. It affects the retention rate of employees.

C. It affects the reputation of an organization.

D. It affects the morale of the employees.

Answer: (SHOW ANSWER)

NEW QUESTION: 144
While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?
A. Trusted path
B. Malicious logic
C. Passive misuse
D. Social engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 145
Which of the following is the PRIMARY issue when collecting detailed log information?
A. Logs may be unavailable when required
B. Timely review of the data is potentially difficult
C. Logs do not provide sufficient details of system and individual activities
D. Most systems and applications do not support logging
Answer: (SHOW ANSWER)

NEW QUESTION: 146
An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?
A. Implement logical network segmentation at the switches
B. Install Host Based Intrusion Detection Systems (HIDS)
C. Require strong authentication for administrators
D. Implement packet filtering on the network firewalls
Answer: (SHOW ANSWER)

NEW QUESTION: 147
What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?
A. Parallel
B. Tabletop
C. Walkthrough
D. Simulation
Answer: (SHOW ANSWER)

NEW QUESTION: 148
As one component of a physical security system, an Electronic Access Control (EAC) token is BEST known for its ability to
A. lock down a facility during an emergency.
B. overcome the problems of key assignments.
C. monitor the opening of windows and doors.
D. trigger alarms when intruders are detected.

Answer: (SHOW ANSWER)

NEW QUESTION: 149
Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?
A. Hypertext Transfer Protocol (HTTP)
B. Lightweight Directory Access Control (LDAP)
C. Security Assertion Markup Language (SAML)
D. Kerberos
Answer: (SHOW ANSWER)

NEW QUESTION: 150
Which of the following is the MOST beneficial to review when performing an IT audit?
A. Security policies
B. Audit policy
C. Configuration settings
D. Security log
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?
A. Confidentiality and Integrity
B. Integrity and Availability
C. Accountability and Assurance
D. Availability and Accountability
Answer: (SHOW ANSWER)

NEW QUESTION: 152
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The third party needs to have
A. processes that are identical to that of the organization doing the outsourcing.
B. access to the skill sets consistent with the programming languages used by the organization.
C. access to the original personnel that were on staff at the organization.
D. the ability to maintain all of the applications in languages they are familiar with.

Answer: (SHOW ANSWER)

NEW QUESTION: 153
During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification.
Which of the following is the MOST likely reason for this?
A. The security requirements have changed during the procurement process.
B. There were no security professionals in the vendor's bidding team.
C. The description of the security requirements was insufficient.
D. The procurement officer lacks technical knowledge.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
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.
Which of the following BEST describes the access control methodology used?
A. Lattice Based Access Control (LBAC)
B. Lightweight Directory Access Control (LDAP)
C. Least privilege
D. Role Based Access Control (RBAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 155
When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?
A. Requirements definition phase
B. Testing phase
C. Development phase
D. Operations and maintenance phase
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Software Code signing is used as a method of verifying what security concept?
A. Confidentiality
B. Integrity
C. Access Control
D. Availability
Answer: (SHOW ANSWER)

NEW QUESTION: 157
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 included in awareness training, and procedures give guidance
C. Policies are generic in nature, and procedures contain operational details
D. Policies point to guidelines, and procedures are more contractual in nature
Answer: (SHOW ANSWER)

NEW QUESTION: 158
Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?
A. Simple Mail Transfer Protocol (SMTP) blacklist
B. Reverse Domain Name System (DNS) lookup
C. Hashing algorithm
D. Header analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 159
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.
Which of the following will be the PRIMARY security concern as staff is released from the organization?
A. Loss of data and separation of duties
B. Inadequate IT support
C. Undocumented security controls
D. Additional responsibilities for remaining staff
Answer: (SHOW ANSWER)

NEW QUESTION: 160
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. ISO/IEC 20000
B. Payment Card Industry Data Security Standard (PCIDSS)
C. International Organization for Standardization (ISO) 27000 family
D. Information Technology Infrastructure Library (ITIL)
Answer: (SHOW ANSWER)

NEW QUESTION: 161
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?
A. As part of the SLA renewal process
B. At regularly scheduled meetings

C. Immediately after a security breach
D. Prior to a planned security audit
Answer: (SHOW ANSWER)

NEW QUESTION: 162
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?
A. The authentication session can be replayed
B. Authorizations are not included in the server response
C. Passwords are passed in cleartext
D. Unsalted hashes are passed over the network
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following is a potential risk when a program runs in privileged mode?
A. It may serve to create unnecessary code complexity
B. It may allow malicious code to be inserted
C. It may not enforce job separation duties
D. It may create unnecessary application hardening
Answer: (SHOW ANSWER)

NEW QUESTION: 164
What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?
A. Identifying the benchmark required for restoration
B. Determining the Recovery Time Objective (RTO)
C. Validating the effectiveness of the plan
D. Evaluating the efficiency of the plan
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Which of the following MUST be done when promoting a security awareness program to senior management?
A. Notify them that their compliance is mandatory
B. Explain how hackers have enhanced information security
C. Ensure that the security presentation is designed to be all-inclusive
D. Show the need for security; identify the message and the audience
Answer: D (LEAVE A REPLY)

NEW QUESTION: 166
Contingency plan exercises are intended to do which of the following?
A. Validate operation metrics
B. Validate service level agreements
C. Train maintenance personnel

D. Train personnel in roles and responsibilities
Answer: (SHOW ANSWER)

NEW QUESTION: 167
Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?
A. Data warehousing
B. Data compression
C. Data classification
D. Data validation
Answer: (SHOW ANSWER)

NEW QUESTION: 168
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.
Which of the following will MOST likely allow the organization to keep risk at an acceptable level?
A. Removing privileged accounts from operational staff
B. Assigning privileged functions to appropriate staff
C. Increasing the amount of audits performed by third parties
D. Separating the security function into distinct roles
Answer: (SHOW ANSWER)

NEW QUESTION: 169
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 the intrusion causes the system processes to hang, which of the following has been affected?
A. System integrity
B. System auditability
C. System confidentiality
D. System availability
Answer: (SHOW ANSWER)

NEW QUESTION: 170

A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

A. The end devices, wireless access points, WLAN, switches, management console, and firewall.
B. The end devices, wireless access points, WLAN, switches, management console, and Internet
C. The entire enterprise network infrastructure.
D. The handheld devices, wireless access points and border gateway.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
Which of the following is most helpful in applying the principle of LEAST privilege?
A. Setting up a Virtual Private Network (VPN) tunnel
B. Monitoring and reviewing privileged sessions
C. Introducing a job rotation program
D. Establishing a sandboxing environment
Answer: (SHOW ANSWER)

NEW QUESTION: 172
An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following MUST be verified by the Information Security Department?
A. The service provider will impose controls and protections that meet or exceed the current systems controls and produce audit logs as verification.
B. The service provider will segregate the data within its systems and ensure that each region's policies are met.
C. The service provider's policies are consistent with ISO/IEC27001 and there is evidence that the service provider is following those policies.
D. The service provider's policies can meet the requirements imposed by the new environment even if they differ from the organization's current policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 173
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 recycled according to NIST SP 800-88.
B. They should be recycled to save energy.
C. They should be inspected and categorized properly to sell them for reuse.
D. They should be inspected and sanitized following the organizational policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 174
Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?
A. Polygraphs, crime statistics, forensics
B. Security control baselines, access controls, employee awareness and training
C. Human resources, asset management, production management

D. Supply chain lead time, inventory control, encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Which of the following types of security testing is the MOST effective in providing a better indication of the everyday security challenges of an organization when performing a security risk assessment?
A. Overt
B. External
C. Internal
D. Covert
Answer: (SHOW ANSWER)

NEW QUESTION: 176
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. audit findings.
B. audit requirements.
C. risk elimination.
D. customer satisfaction.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
Which of the following entities is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider?
A. Data processor
B. Data custodian
C. Data steward
D. Data owner
Answer: (SHOW ANSWER)

NEW QUESTION: 178
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.
In addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?
A. Text editors, database, and Internet phone applications
B. Email, presentation, and database applications
C. Email, media players, and instant messaging applications
D. Image libraries, presentation and spreadsheet applications
Answer: (SHOW ANSWER)

NEW QUESTION: 179

Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

A. Quantifying the system's available services

B. Measuring the system's integrity in the presence of failure

C. Identifying the number of security flaws within the system

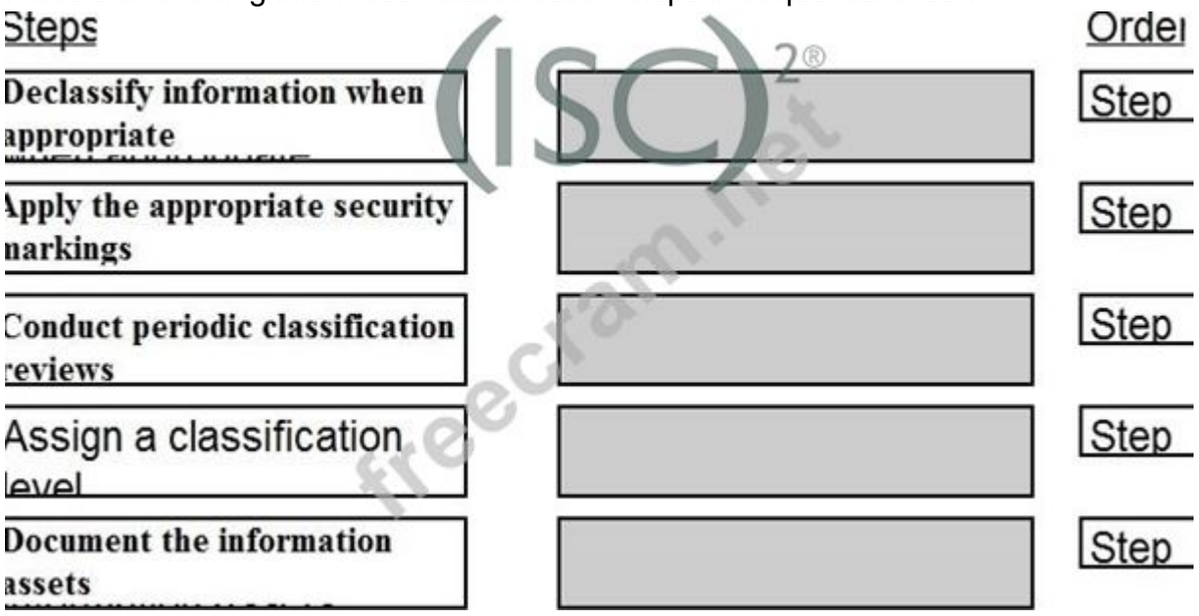
D. Determining the probability that the system functions safely during any time period

Answer: (SHOW ANSWER)

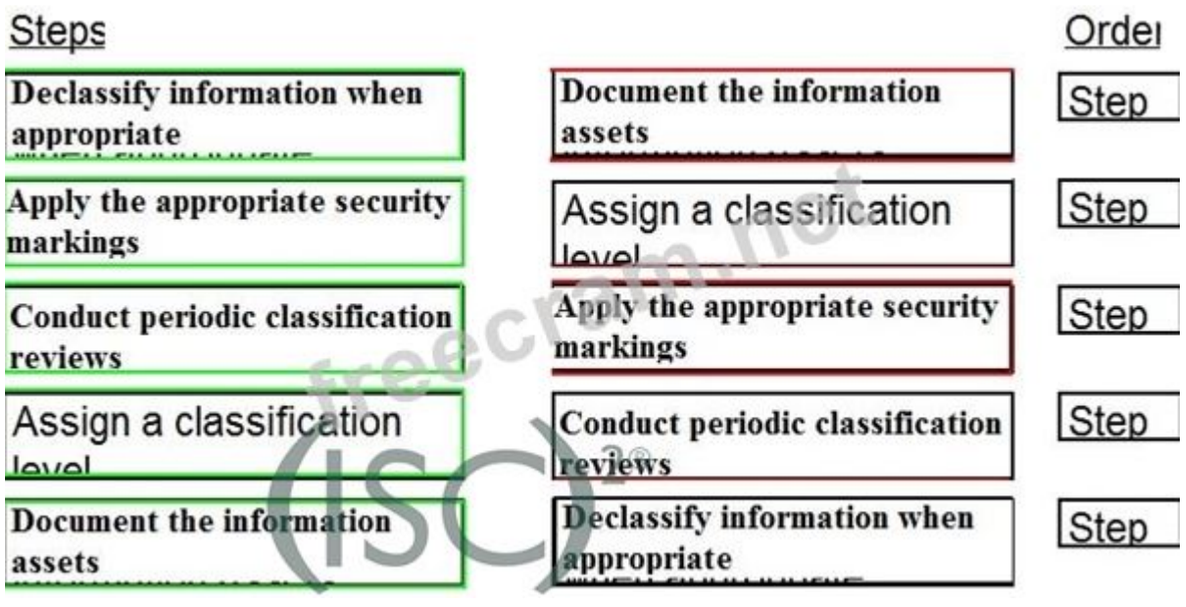
NEW QUESTION: 180

DRAG DROP

Place the following information classification steps in sequential order.



Answer:



NEW QUESTION: 181

After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

A. Use two-factor authentication mechanisms

B. Integrate the VPN with centralized credential stores

C. Implement strong passwords authentication for VPN

D. Implement an Internet Protocol Security (IPSec) client

Answer: A (LEAVE A REPLY)

NEW QUESTION: 182

Which one of the following is a common risk with network configuration management?

A. Patches on the network are difficult to keep current.

B. Network diagrams are not up to date.

C. It is the responsibility of the systems administrator.

D. User ID and passwords are never set to expire.

Answer: (SHOW ANSWER)

NEW QUESTION: 183

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. Asset register

B. Ping testing

C. Mapping tools

D. Topology diagrams

Answer: (SHOW ANSWER)

NEW QUESTION: 184

The stringency of an Information Technology (IT) security assessment will be determined by the

A. sensitivity of the system's data.

B. size of the system's database.

C. age of the system.

D. system's past security record.

Answer: (SHOW ANSWER)

NEW QUESTION: 185

Which item below is a federated identity standard?

A. 802.11i
B. Lightweight Directory Access Protocol (LDAP)
C. Kerberos
D. Security Assertion Markup Language (SAML)
Answer: (SHOW ANSWER)

NEW QUESTION: 186
An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?
A. Covert channel
B. Data emanation
C. Unfiltered channel
D. Data leakage
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Which of the following BEST describes the purpose of performing security certification?
A. To identify system threats, vulnerabilities, and acceptable level of risk
B. To verify that system architecture and interconnections with other systems are effectively implemented
C. To formalize the confirmation of completed risk mitigation and risk analysis
D. To formalize the confirmation of compliance to security policies and standards
Answer: (SHOW ANSWER)

NEW QUESTION: 188
The MAIN reason an organization conducts a security authorization process is to
A. force the organization to make conscious risk decisions.
B. force the organization to enlist management support.
C. assure the effectiveness of security controls.
D. assure the correct security organization exists.
Answer: (SHOW ANSWER)

NEW QUESTION: 189
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 is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?
A. Client hardening and management is easier on clients than on servers.
B. Client-based attacks have higher financial impact.
C. Client-based attacks are more common and easier to exploit than server and network based attacks.
D. Client privilege administration is inherently weaker than server privilege administration.
Answer: (SHOW ANSWER)

NEW QUESTION: 190

When transmitting information over public networks, the decision to encrypt it should be based on

A. the level of confidentiality of the information.

B. the estimated monetary value of the information.

C. the volume of the information.

D. whether there are transient nodes relaying the transmission.

Answer: (SHOW ANSWER)

NEW QUESTION: 191

Which of the following is the BEST solution to provide redundancy for telecommunications links?

A. Provide multiple links from the same telecommunications vendor.

B. Provide multiple links from multiple telecommunications vendors.

C. Ensure that the telecommunications links connect to the network in multiple locations.

D. Ensure that the telecommunications links connect to the network in one location.

Answer: (SHOW ANSWER)

NEW QUESTION: 192

For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

A. Hash functions

B. Non-repudiation controls

C. File system permissions

D. Data segregation

Answer: (SHOW ANSWER)

NEW QUESTION: 193

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

A. Confirm warm site is ready to accept connections.

B. Validate target systems have been backed up.

C. Verify countermeasures have been deactivated.

D. Ensure firewall logging has been activated.

Answer: (SHOW ANSWER)

NEW QUESTION: 194

When constructing an Information Protection Policy (IPP), it is important that the stated rules are necessary, adequate, and

A. flexible.

B. focused.

C. confidential.

D. achievable.

Answer: (SHOW ANSWER)

NEW QUESTION: 195

An advantage of link encryption in a communications network is that it
A. makes key management and distribution easier.
B. protects data from start to finish through the entire network.
C. improves the efficiency of the transmission.
D. encrypts all information, including headers and routing information.
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?
A. Guest users need to authenticate with the third party identity provider.
B. Revocation of access of some users of the third party instead of all the users from the third party.
C. Compromise of the third party means compromise of all the users in the service.
D. Resource Servers are required to use passwords to authenticate end users.
Answer: (SHOW ANSWER)

NEW QUESTION: 197
The 802.1x standard provides a framework for what?
A. Wireless encryption using the Advanced Encryption Standard (AES)
B. Network authentication for wired and wireless networks
C. Wireless network encryption using Secure Sockets Layer (SSL)
D. Network authentication for only wireless networks
Answer: (SHOW ANSWER)

NEW QUESTION: 198
What maintenance activity is responsible for defining, implementing, and testing updates to application systems?
A. Program change control
B. Export exception control
C. Regression testing
D. User acceptance testing
Answer: (SHOW ANSWER)

NEW QUESTION: 199
During a fingerprint verification process, which of the following is used to verify identity and authentication?
A. A hash table is matched to a database of stored value
B. Sets of digits are matched with stored values

C. A pressure value is compared with a stored template

D. A template of minutiae is compared with a stored template

Answer: D (LEAVE A REPLY)

NEW QUESTION: 200

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 data sensitivity.

B. Access is determined by the system.

C. Access is based on user's role.

D. Access is based on rules.

Answer: (SHOW ANSWER)

NEW QUESTION: 201

To protect auditable information, which of the following MUST be configured to only allow read access?

A. Transaction log files

B. Access control lists (ACL)

C. Logging configurations

D. User account configurations

Answer: (SHOW ANSWER)

NEW QUESTION: 202

What is the MOST effective method of testing custom application code?

A. Negative testing

B. White box testing

C. Penetration testing

D. Black box testing

Answer: B (LEAVE A REPLY)

NEW QUESTION: 203

Which of the following is an appropriate source for test data?

A. Test data that has no similarities to production data.

B. Production data that has been sanitized before loading into a test environment.

C. Test data that is mirrored and kept up-to-date with production data.

D. Production data that is secured and maintained only in the production environment.

Answer: (SHOW ANSWER)

NEW QUESTION: 204

To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

A. Multiple-pass overwriting
B. High-level formatting
C. Degaussing
D. Physical destruction
Answer: (SHOW ANSWER)

NEW QUESTION: 205
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 D can write to File 1
B. User B can write to File 1
C. User C can write to File 1
D. User A can write to File 1
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?
A. Knurling
B. Shredding
C. Degaussing
D. Grinding
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?
A. Testing with a Botnet
B. Executing a binary shellcode
C. Testing with an EICAR file
D. Run multiple antivirus programs
Answer: (SHOW ANSWER)

NEW QUESTION: 208
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 expected loss from the risk exceeds mitigation costs.
C. The infrastructure budget can easily cover the upgrade costs.
D. The Annualized Loss Expectancy (ALE) approaches zero.
Answer: (SHOW ANSWER)

NEW QUESTION: 209
The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it
A. exploits weak authentication to penetrate networks.
B. can be detected with signature analysis.
C. looks like normal network activity.
D. is commonly confused with viruses or worms.
Answer: (SHOW ANSWER)

NEW QUESTION: 210
Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

A. Data link encryption
B. Discretionary Access Control (DAC) procedures
C. Segregation of duties
D. Mandatory Access Control (MAC) procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 211
In order for a security policy to be effective within an organization, it MUST include
A. owner information and date of last revision.
B. strong statements that clearly define the problem.
C. a list of all standards that apply to the policy.
D. disciplinary measures for non compliance.
Answer: (SHOW ANSWER)

NEW QUESTION: 212

Which of the following is the BEST mitigation from phishing attacks?
A. Corporate policy and procedures
B. Strong file and directory permissions
C. Network activity monitoring
D. Security awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 213
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?
A. Challenge response and private key
B. Digital certificates and Single Sign-On (SSO)
C. Tokens and passphrase
D. Smart card and biometrics
Answer: (SHOW ANSWER)

NEW QUESTION: 214
What is the PRIMARY advantage of using automated application security testing tools?
A. The application can be protected in the production environment.
B. Large amounts of code can be tested using fewer resources.
C. Detailed testing of code functions can be performed.
D. The application will fail less when tested using these tools.
Answer: (SHOW ANSWER)

NEW QUESTION: 215
Which of the following is the BEST countermeasure to brute force login attacks?
A. Restricting initial password delivery only in person
B. Changing all canonical passwords
C. Introducing a delay after failed system access attempts
D. Decreasing the number of concurrent user sessions
Answer: (SHOW ANSWER)

NEW QUESTION: 216
Why is a system's criticality classification important in large organizations?
A. It provides for easier determination of ownership, reducing confusion as to the status of the asset.
B. It allows for clear systems status communications to executive management.
C. It reduces critical system support workload and reduces the time required to apply patches.
D. It provides for proper prioritization and scheduling of security and maintenance tasks.
Answer: (SHOW ANSWER)

NEW QUESTION: 217

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

NEW QUESTION: 218
Which of the following is an effective method for avoiding magnetic media data remanence?
A. Degaussing
B. Authentication
C. Data Loss Prevention (DLP)
D. Encryption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 219
Internet Protocol (IP) source address spoofing is used to defeat
A. Reverse Address Resolution Protocol (RARP).
B. address-based authentication.
C. Transmission Control Protocol (TCP) hijacking.
D. Address Resolution Protocol (ARP).
Answer: (SHOW ANSWER)

NEW QUESTION: 220
Why must all users be positively identified prior to using multi-user computers?
A. To ensure that management knows what users are currently logged on
B. To provide access to the operating system
C. To ensure that unauthorized persons cannot access the computers
D. To provide access to system privileges
Answer: (SHOW ANSWER)

NEW QUESTION: 221
Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?
A. Cold site
B. Hot site
C. Mobile site
D. Warm site
Answer: A (LEAVE A REPLY)

NEW QUESTION: 222
Which of the following questions can be answered using user and group entitlement reporting?

A. When a particular file was last accessed by a user
B. Where does a particular user have access within the network
C. The number of failed login attempts for a particular user
D. Change control activities for a particular group of users
Answer: (SHOW ANSWER)

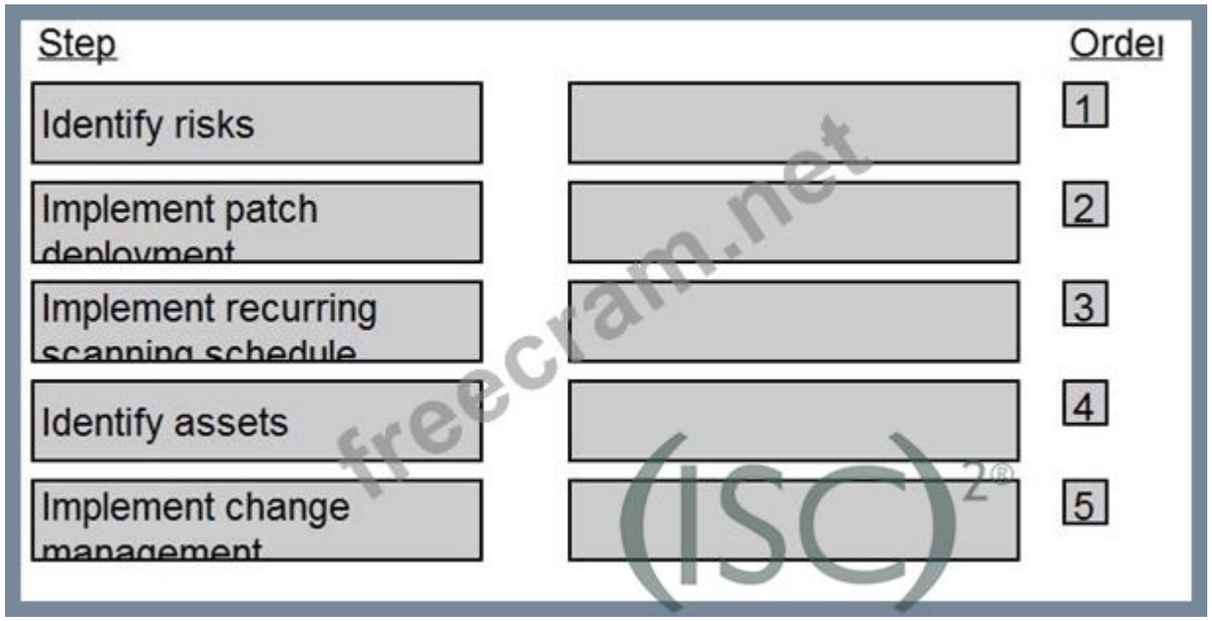
NEW QUESTION: 223
In a basic SYN flood attack, what is the attacker attempting to achieve?
A. Exceed the threshold limit of the connection queue for a given service
B. Cause the buffer to overflow, allowing root access
C. Set the threshold to zero for a given service
D. Flush the register stack, allowing hijacking of the root account
Answer: A (LEAVE A REPLY)

NEW QUESTION: 224
Which of the following is the PRIMARY security concern associated with the implementation of smart cards?
A. The cards can be misplaced
B. Vendor application compatibility
C. Mobile code can be embedded in the card
D. The cards have limited memory
Answer: (SHOW ANSWER)

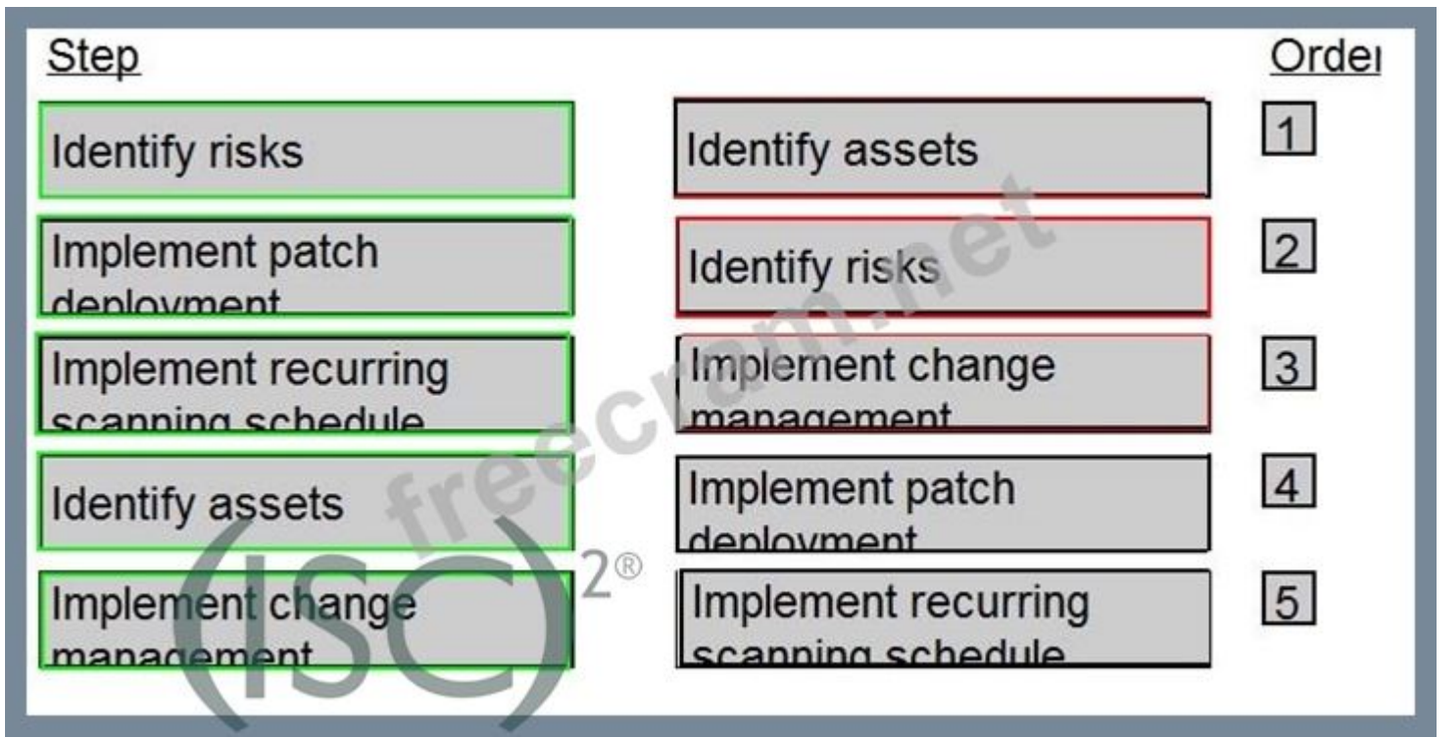
NEW QUESTION: 225
Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?
A. Modification of Certificate Revocation List
B. Delayed revocation or destruction of credentials
C. Token use after decommissioning
D. Unauthorized renewal or re-issuance
Answer: (SHOW ANSWER)

NEW QUESTION: 226
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. Approved web browsers
C. Employee education
D. Network firewall procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 227
DRAG DROP
Order the below steps to create an effective vulnerability management process.



Answer:



NEW QUESTION: 228
Which of the following assures that rules are followed in an identity management architecture?

A. Policy decision point
B. Digital signature
C. Policy database
D. Policy enforcement point
Answer: (SHOW ANSWER)

NEW QUESTION: 229
When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?
A. After the business functional analysis and the data security categorization have been performed
B. After the system preliminary design has been developed and the data security categorization has been performed
C. After the vulnerability analysis has been performed and before the system detailed design begins
D. After the system preliminary design has been developed and before the data security categorization begins
Answer: A (LEAVE A REPLY)

NEW QUESTION: 230
Which of the following describes the concept of a Single Sign-On (SSO) system?
A. Users are identified to multiple systems with several credentials.
B. Users are authenticated to multiple systems with one login.
C. Users are authenticated to one system at a time.
D. Only one user is using the system at a time.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 231
When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include
A. curved roads approaching the data center.
B. hardened building construction with consideration of seismic factors.
C. proximity to high crime areas of the city.
D. adequate distance from and lack of access to adjacent buildings.
Answer: (SHOW ANSWER)

NEW QUESTION: 232
Which one of the following is a threat related to the use of web-based client side input validation?
A. The web server would not be able to receive invalid input from the client
B. The web server would not be able to validate the input after transmission
C. The client system could receive invalid input from the web server
D. Users would be able to alter the input after validation has occurred
Answer: (SHOW ANSWER)

NEW QUESTION: 233
The type of authorized interactions a subject can have with an object is
A. permission.

B. protocol.
C. control.
D. procedure.
Answer: (SHOW ANSWER)

NEW QUESTION: 234
The amount of data that will be collected during an audit is PRIMARILY determined by the
A. availability of the data.
B. audit scope.
C. auditor's experience level.
D. integrity of the data.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 235
Which of the following statements is TRUE of black box testing?
A. Only the source code and functional specifications are known to the test planner.
B. Only the design documents and the functional specifications are known to the test planner.
C. Only the functional specifications are known to the test planner.
D. Only the source code and the design documents are known to the test planner.
Answer: (SHOW ANSWER)

NEW QUESTION: 236
The PRIMARY security concern for handheld devices is the
A. strength of the encryption algorithm.
B. strength of the Personal Identification Number (PIN).
C. spread of malware during synchronization.
D. ability to bypass the authentication mechanism.
Answer: (SHOW ANSWER)

NEW QUESTION: 237
Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?
A. To help the security team accept or reject new systems for implementation and production
B. To assure the software development team that all security issues have been addressed
C. To assist data owners in making future sensitivity and criticality determinations
D. To verify that security protection remains acceptable to the organizational security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 238
Which of the following has the GREATEST impact on an organization's security posture?
A. Resource constraints due to increasing costs of supporting security

B. Audit findings related to employee access and permissions process
C. International and country-specific compliance requirements
D. Security violations by employees and contractors
Answer: C (LEAVE A REPLY)

NEW QUESTION: 239
Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?
A. Avoid storing PII in a Cloud Service Provider.
B. Store PII for no more than one year.
C. Adherence to collection limitation laws and regulations.
D. Encrypt and hash all PII to avoid disclosure and tampering.
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Which of the following methods can be used to achieve confidentiality and integrity for data in transit?
A. Internet Protocol Security (IPSec)
B. Multiprotocol Label Switching (MPLS)
C. Multi-factor authentication
D. Federated identity management
Answer: (SHOW ANSWER)

NEW QUESTION: 241
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

In a Bell-LaPadula system, which user has the MOST restrictions when writing data to any of the four files?
A. User A
B. User C
C. User B
D. User D
Answer: (SHOW ANSWER)

NEW QUESTION: 242
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 ethical because the tool will be used to create a better virus scanner.
B. The behavior is ethical because any experienced programmer could create such a tool.
C. The behavior is not ethical because such a tool could be leaked on the Internet.
D. The behavior is not ethical because creating any kind of virus is bad.
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Following the completion of a network security assessment, which of the following can BEST be demonstrated?
A. A penetration test of the network will fail
B. The network is compliant to industry standards
C. All unpatched vulnerabilities have been identified
D. The effectiveness of controls can be accurately measured
Answer: (SHOW ANSWER)

NEW QUESTION: 244
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. Smurfing
B. Session redirect
C. Man-in-the-Middle (MITM) attack
D. Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 245
How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?
A. Authenticates the IP payload and selected portions of the IP header
B. Encrypts and optionally authenticates the complete IP packet
C. Encrypts and optionally authenticates the IP payload, but not the IP header
D. Encrypts and optionally authenticates the IP header, but not the IP payload
Answer: (SHOW ANSWER)

NEW QUESTION: 246
A large bank deploys hardware tokens to all customers that use their online banking system. The token generates and displays a six digit numeric password every 60 seconds. The customers must log into their bank accounts using this numeric password. This is an example of

A. single factor authentication token.
B. Single Sign-On (SSO) token.
C. asynchronous token.
D. synchronous token.
Answer: (SHOW ANSWER)

NEW QUESTION: 247
What is the FIRST step in developing a security test and its evaluation?
A. Identify all applicable security requirements
B. Develop testing procedures
C. Identify people, processes, and products not in compliance
D. Determine testing methods
Answer: (SHOW ANSWER)

NEW QUESTION: 248
What is the process called when impact values are assigned to the security objectives for information types?
A. System security categorization
B. Remediation
C. Qualitative analysis
D. Quantitative analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 249
Which of the following explains why record destruction requirements are included in a data retention policy?
A. To validate data ownership
B. To save cost for storage and backup
C. To comply with legal and business requirements
D. To meet destruction guidelines
Answer: (SHOW ANSWER)

NEW QUESTION: 250
Which of the following command line tools can be used in the reconnaisance phase of a network vulnerability assessment?

A. dig
B. ipconfig
C. ifconfig
D. nbtstat
Answer: (SHOW ANSWER)

NEW QUESTION: 251
Which of the following is a detective access control mechanism?

A. Least privilege
B. Password complexity
C. Log review
D. Non-disclosure agreement
Answer: (SHOW ANSWER)

NEW QUESTION: 252
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.
In addition to authentication at the start of the user session, best practice would require re-authentication
A. at system sign-off.
B. for each business process.
C. after a period of inactivity.
D. periodically during a session.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 253
A practice that permits the owner of a data object to grant other users access to that object would usually provide
A. owner-administered control.
B. owner-dependent access control.
C. Mandatory Access Control (MAC).
D. Discretionary Access Control (DAC).
Answer: (SHOW ANSWER)

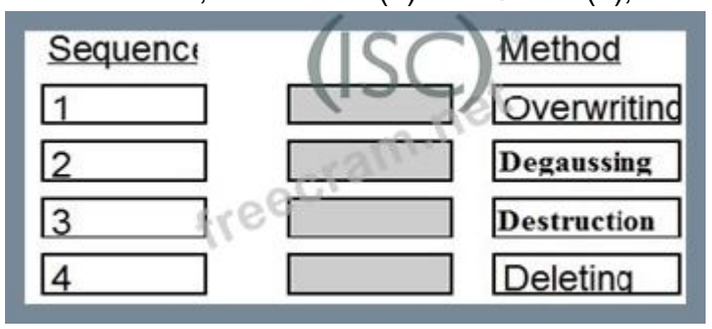
NEW QUESTION: 254
A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?
A. Random number generator
B. Encryption routines
C. Botnet command and control
D. Obfuscated code
Answer: (SHOW ANSWER)

NEW QUESTION: 255
What component of a web application that stores the session state in a cookie can be bypassed by an attacker?
A. An identification check
B. An initialization check
C. An authorization check
D. An authentication check
Answer: (SHOW ANSWER)

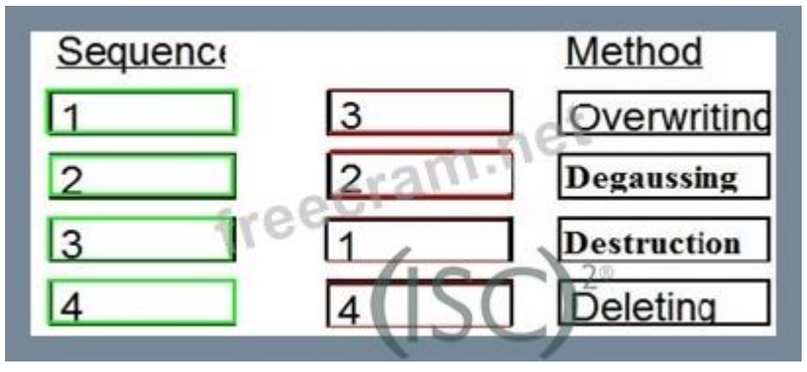
NEW QUESTION: 256
Which of the following BEST represents the principle of open design?
A. Disassembly, analysis, or reverse engineering will reveal the security functionality of the computer system.
B. A knowledgeable user should have limited privileges on the system to prevent their ability to compromise security capabilities.
C. The security of a mechanism should not depend on the secrecy of its design or implementation.
D. Algorithms must be protected to ensure the security and interoperability of the designed system.
Answer: (SHOW ANSWER)

NEW QUESTION: 257
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. Limits and scope of the testing.
B. Employee directory and organizational chart.
C. Logical location of filters and concentrators.
D. Physical location of server room and wiring closet.
Answer: (SHOW ANSWER)

NEW QUESTION: 258
DRAG DROP
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic media.



Answer:



NEW QUESTION: 259
The FIRST step in building a firewall is to
A. identify mechanisms to encourage compliance with the policy.
B. perform a risk analysis to identify issues to be addressed.
C. define the intended audience who will read the firewall policy.
D. assign the roles and responsibilities of the firewall administrators.
Answer: (SHOW ANSWER)

NEW QUESTION: 260
A security manager has noticed an inconsistent application of server security controls resulting in vulnerabilities on critical systems. What is the MOST likely cause of this issue?

A. A poorly designed security policy communication program
B. A lack of baseline standards
C. Host-based Intrusion Prevention System (HIPS) policies are ineffective
D. Improper documentation of security guidelines
Answer: (SHOW ANSWER)

NEW QUESTION: 261
An organization is designing a large enterprise-wide document repository system. They plan to have several different classification level areas with increasing levels of controls. The BEST way to ensure document confidentiality in the repository is to
A. utilize Intrusion Detection System (IDS) set drop connections if too many requests for documents are detected.
B. require individuals with access to the system to sign Non-Disclosure Agreements (NDA).
C. encrypt the contents of the repository and document any exceptions to that requirement.
D. keep individuals with access to high security areas from saving those documents into lower security areas.
Answer: (SHOW ANSWER)

NEW QUESTION: 262
Which one of the following describes granularity?
A. Number of violations divided by the number of total accesses
B. Fineness to which a trusted system can authenticate users
C. Fineness to which an access control system can be adjusted
D. Maximum number of entries available in an Access Control List (ACL)
Answer: (SHOW ANSWER)

NEW QUESTION: 263
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.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?
A. Severity of risk

B. Ongoing awareness
C. Frequency of incidents
D. Complexity of strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 264
Are companies legally required to report all data breaches?
A. No, different jurisdictions have different rules.
B. No, companies' codes of ethics don't require it.
C. No, not if the data is encrypted.
D. No, only if the breach had a material impact.
Answer: (SHOW ANSWER)

NEW QUESTION: 265
Which of the following is an authentication protocol in which a new random number is generated uniquely for each login session?
A. Point-to-Point Protocol (PPP)
B. Extensible Authentication Protocol (EAP)
C. Password Authentication Protocol (PAP)
D. Challenge Handshake Authentication Protocol (CHAP)
Answer: (SHOW ANSWER)

NEW QUESTION: 266
When using third-party software developers, which of the following is the MOST effective method of providing software development Quality Assurance (QA)?
A. Retain intellectual property rights through contractual wording.
B. Perform overlapping code reviews by both parties.
C. Verify that the contractors attend development planning meetings.
D. Create a separate contractor development environment.
Answer: (SHOW ANSWER)

NEW QUESTION: 267
Which of the following BEST describes a Protection Profile (PP)?
A. A document that is used to develop an IT security product from its security requirements definition.
B. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).
C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
D. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
Answer: (SHOW ANSWER)

NEW QUESTION: 268
An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?
A. A backdoor installation

B. A dictionary attack
C. A Denial of Service (DoS) attack
D. A spoofing attack
Answer: (SHOW ANSWER)

NEW QUESTION: 269
Which of the following is the best practice for testing a Business Continuity Plan (BCP)?
A. Test after installation of security patches
B. Test when environment changes
C. Test before the IT Audit
D. Test after implementation of system patches
Answer: (SHOW ANSWER)

NEW QUESTION: 270
A thorough review of an organization's audit logs finds that a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient. What type of attack has MOST likely occurred?

A. Man-in-the-middle
B. Denial of service
C. Eavesdropping
D. Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 271
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. Denial of Service (DoS)
B. Trojan horse
C. Spoofing
D. Man-in-the-Middle (MITM)
Answer: (SHOW ANSWER)

NEW QUESTION: 272
The PRIMARY outcome of a certification process is that it provides documented
A. security analyses needed to make a risk-based decision.

B. standards for security assessment, testing, and process evaluation.
C. interconnected systems and their implemented security controls.
D. system weaknesses for remediation.
Answer: (SHOW ANSWER)

NEW QUESTION: 273
In a financial institution, who has the responsibility for assigning the classification to a piece of information?
A. Chief Information Security Officer (CISO)
B. Originator or nominated owner of the information
C. Chief Financial Officer (CFO)
D. Department head responsible for ensuring the protection of the information
Answer: (SHOW ANSWER)

NEW QUESTION: 274
Copyright provides protection for which of the following?
A. Ideas expressed in literary works
B. A particular expression of an idea
C. Discoveries of natural phenomena
D. New and non-obvious inventions
Answer: (SHOW ANSWER)

NEW QUESTION: 275
Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?
A. Countermeasures and mitigations for vulnerabilities
B. Application interface entry and endpoints
C. The likelihood and impact of a vulnerability
D. A data flow diagram for the application and attack surface analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 276
Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?
A. Passwords with alpha-numeric and special characters
B. Timed sessions and Secure Socket Layer (SSL)
C. Digital certificates and hardware tokens
D. Two-factor authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 277
Disaster Recovery Plan (DRP) training material should be
A. stored in a fire proof safe to ensure availability when needed.

B. consistent so that all audiences receive the same training.
C. presented in a professional looking manner.
D. only delivered in paper format.
Answer: (SHOW ANSWER)

NEW QUESTION: 278
Who must approve modifications to an organization's production infrastructure configuration?
A. System operations
B. System users
C. Change control board
D. Technical management
Answer: (SHOW ANSWER)

NEW QUESTION: 279
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. Security procedures
B. Human resource standards
C. Human resource policy
D. Security standards
Answer: (SHOW ANSWER)

NEW QUESTION: 280
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

A. Escalation
B. Communication
C. Planning
D. Recovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 281
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: 282
What is the PRIMARY goal for using Domain Name System Security Extensions (DNSSEC) to sign records?
A. Confidentiality
B. Accountability
C. Availability
D. Integrity
Answer: (SHOW ANSWER)

NEW QUESTION: 283
Which of the following is an example of two-factor authentication?
A. Fingerprint and a smart card
B. Password and Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)
C. Magnetic stripe card and an ID badge
D. Retina scan and a palm print
Answer: (SHOW ANSWER)

NEW QUESTION: 284
Why MUST a Kerberos server be well protected from unauthorized access?
A. It always operates at root privilege.
B. It contains the Internet Protocol (IP) address of all network entities.
C. It contains all the tickets for services.
D. It contains the keys of all clients.
Answer: (SHOW ANSWER)

NEW QUESTION: 285
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?
A. Connect the laptop only to well-known networks like the hotel or public Internet cafes.
B. Do not take unnecessary information, including sensitive information.
C. Request international points of contact help scan the laptop on arrival to ensure it is protected.
D. Use a thumb drive to transfer information from a foreign computer.
Answer: (SHOW ANSWER)

NEW QUESTION: 286
Which of the following actions should be performed when implementing a change to a database schema in a production system?
A. Apply change to production, run in parallel, finalize change in production, and develop a back-out strategy
B. Change in development, perform user acceptance testing, develop a back-out strategy, and implement change
C. Perform user acceptance testing in production, have users sign off, and finalize change
D. Test in development, determine dates, notify users, and implement in production
Answer: (SHOW ANSWER)

NEW QUESTION: 287
Which one of the following transmission media is MOST effective in preventing data interception?
A. Fiber optic
B. Coaxial cable
C. Twisted-pair
D. Microwave
Answer: (SHOW ANSWER)

NEW QUESTION: 288
Which of the following BEST describes a rogue Access Point (AP)?
A. An AP connected to the wired infrastructure but not under the management of authorized network administrators
B. An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data Encryption Algorithm (3DES)
C. An AP that is not protected by a firewall
D. An AP infected by any kind of Trojan or Malware
Answer: (SHOW ANSWER)

NEW QUESTION: 289
What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?
A. Procedures in systems development
B. Definition of security profiles
C. Human resource planning efforts
D. Experience in the industry
Answer: (SHOW ANSWER)

NEW QUESTION: 290
When planning a penetration test, the tester will be MOST interested in which information?
A. Job application handouts and tours
B. Places to install back doors
C. Exploits that can attack weaknesses
D. The main network access points
Answer: (SHOW ANSWER)

NEW QUESTION: 291
According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?
A. Disaster Recovery (DR) Team

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

NEW QUESTION: 292
Multi-threaded applications are more at risk than single-threaded applications to
A. packet sniffing.
B. virus infection.
C. database injection.
D. race conditions.
Answer: (SHOW ANSWER)

NEW QUESTION: 293
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
What additional considerations are there if the third party is located in a different country?
A. The effects of transborder data flows and customer expectations regarding the storage or processing of their data
B. The ability of the third party to respond to the organization in a timely manner and with accurate information
C. The organizational structure of the third party and how it may impact timelines within the organization
D. The quantity of data that must be provided to the third party and how it is to be used
Answer: (SHOW ANSWER)

NEW QUESTION: 294
Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy
contain?
A. An explanation of the regulatory frameworks and compliance standards the information collecting organization adheres to.
B. An explanation of all the technologies employed by the collecting organization in gathering information on the data subject.
C. An explanation of who can be contacted at the organization collecting the information if corrections are required by the data subject.
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: 295
Which methodology is recommended for penetration testing to be effective in the development phase of the life-cycle process?
A. Software fuzz testing
B. Black-box testing
C. White-box testing
D. Visual testing
Answer: (SHOW ANSWER)

NEW QUESTION: 296
In Business Continuity Planning (BCP), what is the importance of documenting business processes?
A. Defines who will perform which functions during a disaster or emergency
B. Provides an understanding of the organization's interdependencies
C. Provides senior management with decision-making tools
D. Establishes and adopts ongoing testing and maintenance strategies
Answer: (SHOW ANSWER)

NEW QUESTION: 297
What is the MOST critical factor to achieve the goals of a security program?
A. Executive management support
B. Budget approved for security resources
C. Effectiveness of security management
D. Capabilities of security resources
Answer: (SHOW ANSWER)

NEW QUESTION: 298
What is the ultimate objective of information classification?
A. To ensure that information assets receive an appropriate level of protection
B. To recognize the optimal number of classification categories and the benefits to be gained from their use
C. To recognize that the value of any item of information may change over time
D. To assign responsibility for mitigating the risk to vulnerable systems
Answer: (SHOW ANSWER)

NEW QUESTION: 299
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. Use Secure Sockets Layer (SSL) VPN technology.
B. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.
C. Use Secure Shell (SSH) with public/private keys.
D. Require students to purchase home router capable of VPN.
Answer: (SHOW ANSWER)

NEW QUESTION: 300
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.
Which of the following is considered the MOST important priority for the information security officer?

A. Audit of all organization system configurations for faults
B. Disciplinary actions taken against unethical behavior
C. Development of an awareness program for new employees

D. Formal acceptance of the security strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 301
Which of the following is a recommended alternative to an integrated email encryption system?
A. Sign emails containing sensitive data
B. Encrypt sensitive data separately in attachments
C. Store sensitive information to be sent in encrypted drives
D. Send sensitive data in separate emails
Answer: (SHOW ANSWER)

NEW QUESTION: 302
Which of the following is the PRIMARY benefit of implementing data-in-use controls?
A. When the data is being viewed, it must be accessed using secure protocols.
B. If the data is lost, it will not be accessible to unauthorized users.
C. When the data is being viewed, it can only be printed by authorized users.
D. If the data is lost, it must be decrypted to be opened.
Answer: (SHOW ANSWER)

NEW QUESTION: 303
Data leakage of sensitive information is MOST often concealed by which of the following?
A. Wired Equivalent Privacy (WEP)
B. Secure Sockets Layer (SSL)
C. Secure Hash Algorithm (SHA)
D. Secure Post Office Protocol (POP)
Answer: (SHOW ANSWER)

NEW QUESTION: 304
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. Insufficient Service Level Agreement (SLA)
B. Absence of a Business Intelligence (BI) solution
C. Inadequate cost modeling
D. Improper deployment of the Service-Oriented Architecture (SOA)
Answer: (SHOW ANSWER)

NEW QUESTION: 305
Which of the following is the FIRST step of a penetration test plan?
A. Scheduling the penetration test during a period of least impact
B. Notifying the company's customers
C. Analyzing a network diagram of the target network
D. Obtaining the approval of the company's management
Answer: (SHOW ANSWER)

NEW QUESTION: 306
An organization's data policy MUST include a data retention period which is based on
A. regulatory compliance.
B. digital certificates expiration.
C. business procedures.
D. application dismissal.
Answer: (SHOW ANSWER)

NEW QUESTION: 307
Which of the following actions MUST be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?
A. Monitor the application and review code.
B. Make changes following principle and design guidelines.
C. Stop the application until the vulnerability is fixed.
D. Report the vulnerability to product owner.
Answer: (SHOW ANSWER)

NEW QUESTION: 308
Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?
A. Encrypt the virtual drive where confidential files can be stored
B. Encrypt the entire disk and delete contents after a set number of failed access attempts
C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
D. Set up a BIOS and operating system password
Answer: (SHOW ANSWER)

NEW QUESTION: 309
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. Recovery
B. Reporting
C. Remediation
D. Retention
Answer: (SHOW ANSWER)

NEW QUESTION: 310
Which of the following BEST describes Recovery Time Objective (RTO)?
A. Time of application resumption after disaster
B. Time of application verification after disaster
C. Time of data validation after disaster
D. Time of data restoration from backup after disaster
Answer: (SHOW ANSWER)

NEW QUESTION: 311
Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?
A. Terminate the penetration test and pass the finding to the server management team
B. Continue the testing to its completion and then inform IT management
C. Immediately document the finding and report to senior management.
D. Use system privileges to alter the permissions to secure the server
Answer: (SHOW ANSWER)

NEW QUESTION: 312
A vulnerability test on an Information System (IS) is conducted to
A. measure system performance on systems with weak security controls.
B. evaluate the effectiveness of security controls.
C. prepare for Disaster Recovery (DR) planning.
D. exploit security weaknesses in the IS.
Answer: (SHOW ANSWER)

NEW QUESTION: 313
Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?
A. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
B. Acquisition, Measurement, Configuration Management, Production, Operation, Support
C. Concept, Development, Production, Utilization, Support, Retirement
D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal
Answer: (SHOW ANSWER)

NEW QUESTION: 314
The BEST example of the concept of "something that a user has" when providing an authorized user access to a computing system is
A. the user's hand geometry.
B. a credential stored in a token.
C. a passphrase.
D. the user's face.
Answer: (SHOW ANSWER)

NEW QUESTION: 315
During an audit of system management, auditors find that the system administrator has not been trained. What actions need to be taken at once to ensure the integrity of systems?
A. A review of all systems by an experienced administrator
B. A review of all training procedures to be undertaken
C. A review of all departmental procedures
D. A review of hiring policies and methods of verification of new employees
Answer: A (LEAVE A REPLY)

NEW QUESTION: 316
Which of the following is an essential element of a privileged identity lifecycle management?
A. Regularly perform account re-validation and approval
B. Frequently review performed activities and request justification
C. Account information to be provided by supervisor or line manager
D. Account provisioning based on multi-factor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 317
Which of the following is the MOST important element of change management documentation?
A. List of components involved
B. A stakeholder communication
C. Business case justification
D. Number of changes being made
Answer: (SHOW ANSWER)

NEW QUESTION: 318
Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?
A. Volume encryption
B. Data tokenization
C. Transparent Database Encryption (TDE)
D. Column level database encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 319
Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

A. Write a Service Level Agreement (SLA) for the two companies.
B. Set up a Virtual Private Network (VPN) between the two companies.
C. Establish a File Transfer Protocol (FTP) connection between the two companies.
D. Configure a firewall at the perimeter of each of the two companies.
Answer: (SHOW ANSWER)

NEW QUESTION: 320
During an audit, the auditor finds evidence of potentially illegal activity. Which of the following is the MOST appropriate action to take?

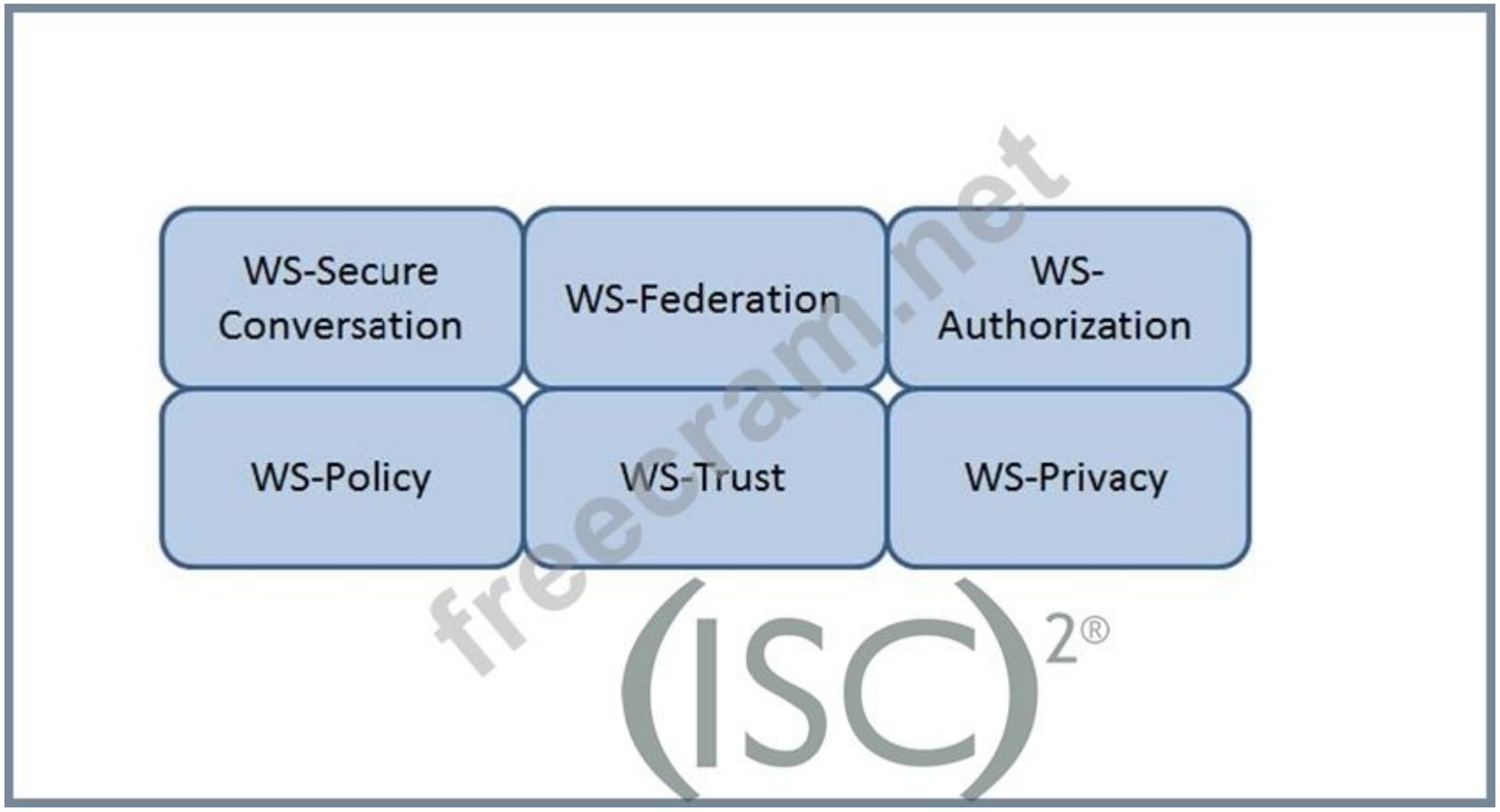
A. Advise the person performing the illegal activity to cease and desist
B. Work with the client to report the activity to the appropriate authority
C. Work with the client to resolve the issue internally
D. Immediately call the police
Answer: (SHOW ANSWER)

NEW QUESTION: 321
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?
A. Validate the service provider's PCI-DSS compliance status on a regular basis.
B. Perform a service provider PCI-DSS assessment on a yearly basis.
C. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis.
D. Validate that the service providers security policies are in alignment with those of the organization.
Answer: (SHOW ANSWER)

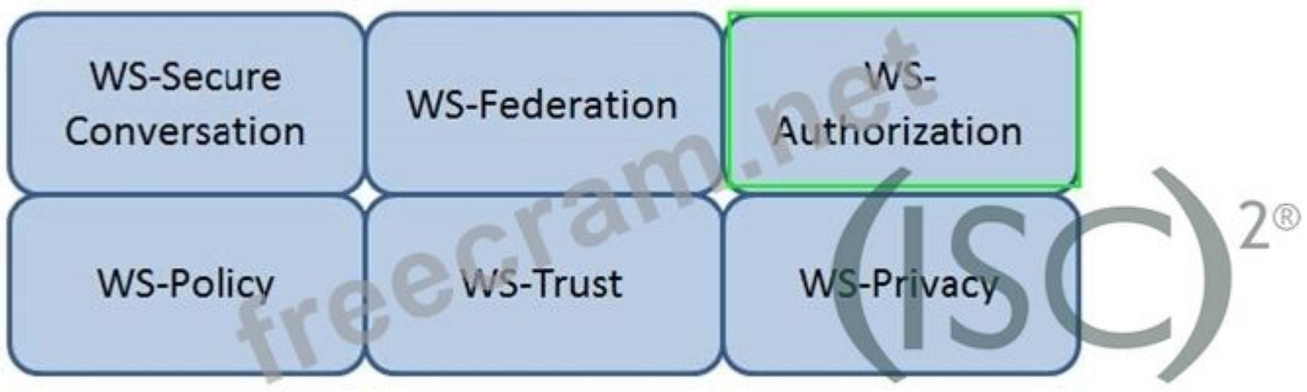
NEW QUESTION: 322
Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?
A. Brute force, dictionary, phishing, keylogger
B. Zeus, netbus, rabbit, turtle
C. Masquerading, salami, malware, polymorphism
D. Token, biometrics, IDS, DLP
Answer: (SHOW ANSWER)

NEW QUESTION: 323
Which of the following is the PRIMARY benefit of a formalized information classification program?
A. It minimizes system logging requirements.
B. It reduces asset vulnerabilities.
C. It drives audit processes.
D. It supports risk assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 324
HOTSPOT
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:



NEW QUESTION: 325
Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?
A. Interface with the Public Key Infrastructure (PKI)
B. Improve the quality of security software
C. Establish a secure initial state
D. Prevent Denial of Service (DoS) attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 326
Which of the following is the BEST reason to review audit logs periodically?
A. Verify they are operating properly
B. Meet compliance regulations
C. Monitor employee productivity
D. Identify anomalies in use patterns
Answer: (SHOW ANSWER)

NEW QUESTION: 327
An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?
A. Customer makes request to retain
B. Long term data mining needs
C. Useful for future business initiatives
D. Pending legal hold
Answer: (SHOW ANSWER)

NEW QUESTION: 328
Which of the following does the Encapsulating Security Payload (ESP) provide?
A. Integrity and confidentiality
B. Availability and integrity
C. Authorization and integrity
D. Authorization and confidentiality
Answer: (SHOW ANSWER)

NEW QUESTION: 329
Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?
A. IEEE 802.1H
B. IEEE 802.1X
C. IEEE 802.1Q
D. IEEE 802.1F

Answer: (SHOW ANSWER)

NEW QUESTION: 330

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. Remediation of vulnerabilities
C. Adoption of standardized policies and procedures
D. Acceptance of risk by the authorizing official
Answer: (SHOW ANSWER)

NEW QUESTION: 331

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.
Which of the following will indicate where the IT budget is BEST allocated during this time?
A. Guidelines
B. Metrics
C. Policies
D. Frameworks
Answer: (SHOW ANSWER)

NEW QUESTION: 332

Which of the following is a function of Security Assertion Markup Language (SAML)?
A. Extended validation
B. File allocation
C. Redundancy check
D. Policy enforcement
Answer: (SHOW ANSWER)

NEW QUESTION: 333

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.

Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?
A. Availability of the database
B. Integrity of security logs
C. Confidentiality of the incident
D. Unauthorized database changes
Answer: (SHOW ANSWER)

NEW QUESTION: 334
Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?
A. Selection to meet the security objectives stated in test documents
B. Definition of the roles and responsibilities
C. Level of assurance of the Target of Evaluation (TOE) in intended operational environment
D. Security behavior expected of a TOE
Answer: (SHOW ANSWER)

NEW QUESTION: 335
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 Creator
C. Data User
D. Data Custodian
Answer: (SHOW ANSWER)

NEW QUESTION: 336
During an investigation of database theft from an organization's web site, it was determined that the Structured Query Language (SQL) injection technique was used despite input validation with client-side scripting. Which of the following provides the GREATEST protection against the same attack occurring again?
A. Encrypt the web server traffic
B. Implement server-side filtering
C. Filter outgoing traffic at the perimeter firewall
D. Encrypt communications between the servers
Answer: (SHOW ANSWER)

NEW QUESTION: 337
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?
A. Tactical, strategic, and financial
B. Documentation, observation, and manual
C. Management, operational, and technical
D. Standards, policies, and procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 338
How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?
A. Take another backup of the media in question then delete all irrelevant operating system files.
B. Create a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level.
C. Discard harmless files for the operating system, and known installed programs.
D. Generate a message digest (MD) or secure hash on the drive image to detect tampering of the media being examined.
Answer: (SHOW ANSWER)

NEW QUESTION: 339
Which of the following does Temporal Key Integrity Protocol (TKIP) support?
A. Multicast and broadcast messages
B. Wired Equivalent Privacy (WEP) systems
C. Synchronization of multiple devices
D. Coordination of IEEE 802.11 protocols
Answer: (SHOW ANSWER)

NEW QUESTION: 340
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.
In the plan, what is the BEST approach to mitigate future internal client-based attacks?

A. Screen for harmful exploits of client-side services before implementation.
B. Harden the client image before deployment.
C. Block all client side web exploits at the perimeter.
D. Remove all non-essential client-side web services from the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 341
In a data classification scheme, the data is owned by the
A. end users.
B. system security managers.
C. Information Technology (IT) managers.
D. business managers.
Answer: (SHOW ANSWER)

NEW QUESTION: 342
Logical access control programs are MOST effective when they are
A. maintained by computer security officers.
B. approved by external auditors.
C. made part of the operating system.
D. combined with security token technology.

Answer: (SHOW ANSWER)

NEW QUESTION: 343
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 business purpose for which the data is to be used
B. Secondary use of the data by business users
C. The overall protection of corporate resources and data
D. The organization's security policies and standards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 344
A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?
A. Identify and select recovery strategies.
B. Present the findings to management for funding.
C. Prepare a plan to test the organization's ability to recover its operations.
D. Select members for the organization's recovery teams.
Answer: (SHOW ANSWER)

NEW QUESTION: 345
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?
A. Development and Deployment
B. Production Operations
C. Utilization Support
D. Requirements Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 346
The birthday attack is MOST effective against which one of the following cipher technologies?
A. Chaining block encryption
B. Streaming cryptography
C. Asymmetric cryptography
D. Cryptographic hash
Answer: (SHOW ANSWER)

NEW QUESTION: 347
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?
A. Data-Link
B. Session
C. Transport
D. Physical
Answer: (SHOW ANSWER)

NEW QUESTION: 348
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. Key Distribution Center (KDC)
C. Simple Key-Management for Internet Protocol (SKIP)
D. Trusted Platform Module (TPM)
Answer: (SHOW ANSWER)

NEW QUESTION: 349
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?
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?
A. Document the system as high risk
B. Perform a vulnerability assessment
C. Notate the information and move on
D. Perform a quantitative threat assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 350
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. automatically compensate for variance in background temperature.

C. reduce the detected object temperature in relation to the background temperature.
D. increase the detected object temperature in relation to the background temperature.
Answer: (SHOW ANSWER)

NEW QUESTION: 351
Which of the following statements is TRUE for point-to-point microwave transmissions?
A. They are subject to interception by an antenna within proximity.
B. They are not subject to interception due to encryption.
C. Interception only depends on signal strength.
D. They are too highly multiplexed for meaningful interception.
Answer: (SHOW ANSWER)

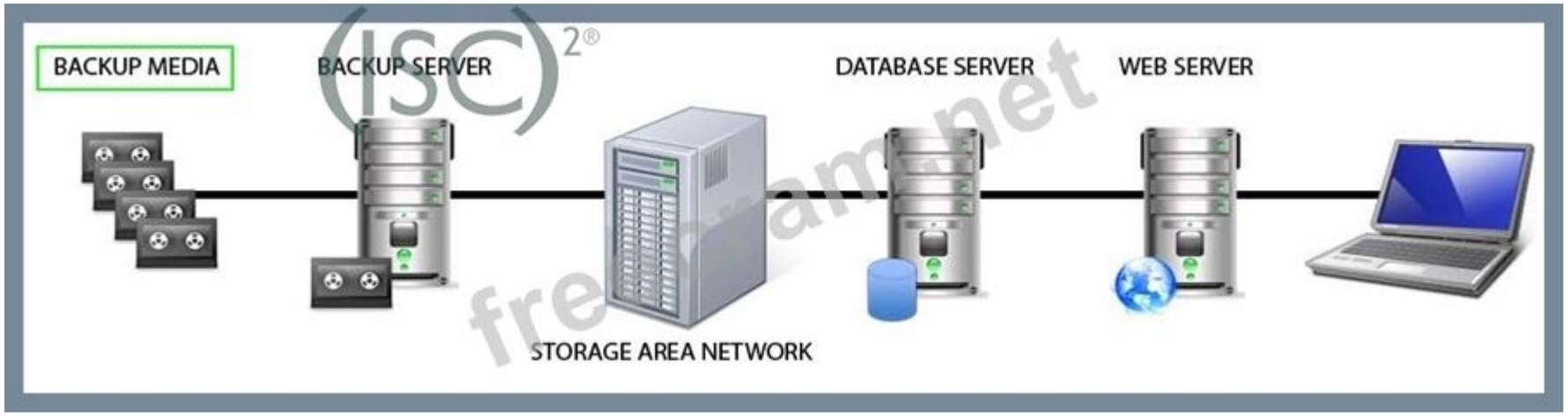
NEW QUESTION: 352
What is the MOST effective countermeasure to a malicious code attack against a mobile system?
A. Sandbox
B. Memory management
C. Public-Key Infrastructure (PKI)
D. Change control
Answer: (SHOW ANSWER)

NEW QUESTION: 353
Which security action should be taken FIRST when computer personnel are terminated from their jobs?
A. Conduct an exit interview
B. Require them to turn in their badge
C. Reduce their physical access level to the facility
D. Remove their computer access
Answer: (SHOW ANSWER)

NEW QUESTION: 354
Which of the following is a network intrusion detection technique?
A. Port scanning
B. Network spoofing
C. Perimeter intrusion
D. Statistical anomaly
Answer: D (LEAVE A REPLY)

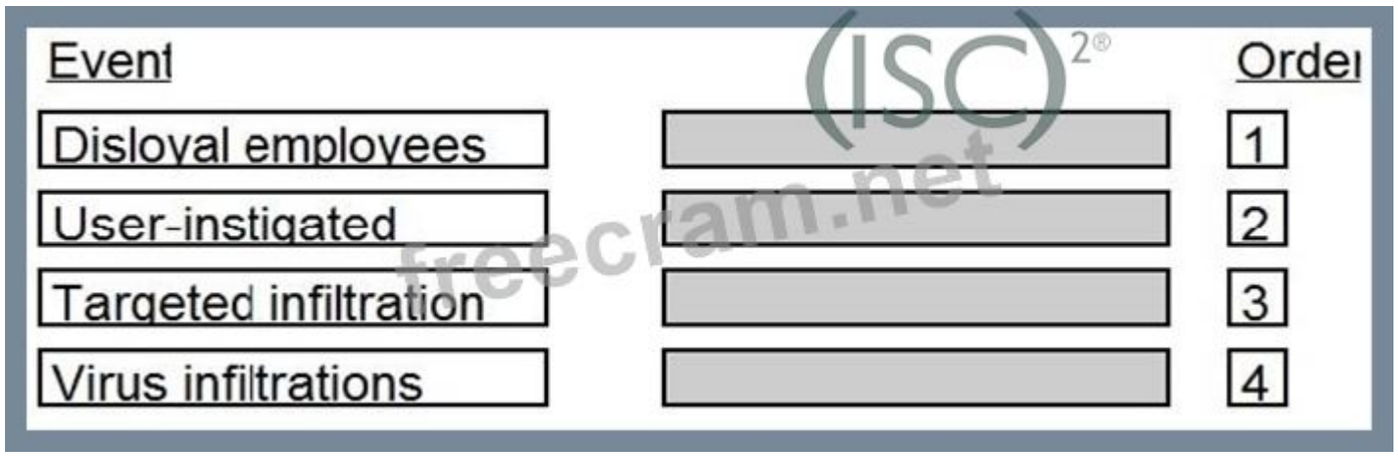
NEW QUESTION: 355
HOTSPOT
Identify the component that MOST likely lacks digital accountability related to information access.
Click on the correct device in the image below.

Answer:

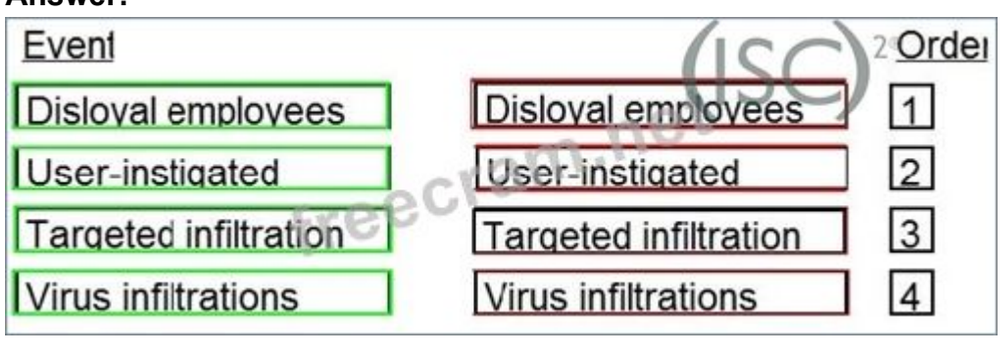


NEW QUESTION: 356
Which of the following is an advantage of on-premise Credential Management Systems?
A. Lower infrastructure capital costs
B. Control over system configuration
C. Reduced administrative overhead
D. Improved credential interoperability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 357
DRAG DROP
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?



Answer:



NEW QUESTION: 358

Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.

Which of the following could have MOST likely prevented the Peer-to-Peer (P2P) program from being installed on the computer?

A. Supervising their child's use of the computer

B. Limiting computer's access to only the employee

C. Ensuring employee understands their business conduct guidelines

D. Removing employee's full access to the computer

Answer: (SHOW ANSWER)

NEW QUESTION: 359

Which of the following is required to determine classification and ownership?

A. System security controls are fully integrated

B. Data file references are identified and linked

C. System and data resources are properly identified

D. Access violations are logged and audited

Answer: (SHOW ANSWER)

NEW QUESTION: 360

The overall goal of a penetration test is to determine a system's

A. error recovery capabilities.

B. capacity management.
C. ability to withstand an attack.
D. reliability under stress.
Answer: (SHOW ANSWER)

NEW QUESTION: 361
Which of the following is the BEST way to verify the integrity of a software patch?
A. Version numbering
B. Cryptographic checksums
C. Vendor assurance
D. Automatic updates
Answer: (SHOW ANSWER)

NEW QUESTION: 362
What principle requires that changes to the plaintext affect many parts of the ciphertext?
A. Obfuscation
B. Encapsulation
C. Permutation
D. Diffusion
Answer: D (LEAVE A REPLY)

NEW QUESTION: 363
Which of the following is a reason to use manual patch installation instead of automated patch management?
A. The ability to cover large geographic areas is increased.
B. The time during which systems will remain vulnerable to an exploit will be decreased.
C. The likelihood of system or application incompatibilities will be decreased.
D. The cost required to install patches will be reduced.
Answer: (SHOW ANSWER)

NEW QUESTION: 364
When implementing controls in a heterogeneous end-point network for an organization, it is critical that
A. users can make modifications to their security software configurations.
B. common software security components be implemented across all hosts.
C. firewalls running on each host are fully customizable by the user.
D. hosts are able to establish network communications.

Answer: (SHOW ANSWER)

NEW QUESTION: 365
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. cost benefit analysis.
B. security impact analysis.
C. routine self assessment.
D. structured code review.
Answer: (SHOW ANSWER)

NEW QUESTION: 366
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

In a Bell-LaPadula system, which user cannot write to File 3?
A. User D
B. User C
C. User A
D. User B
Answer: (SHOW ANSWER)

NEW QUESTION: 367
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The organization should ensure that the third party's physical security controls are in place so that they
A. allow access by the organization staff at any time.
B. are able to limit access to sensitive information.
C. cannot be accessed by subcontractors of the third party.
D. are more rigorous than the original controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 368
The BEST method to mitigate the risk of a dictionary attack on a system is to
A. implement password history.
B. encrypt the access control list (ACL).

C. use complex passphrases.
D. use a hardware token.
Answer: (SHOW ANSWER)

NEW QUESTION: 369
An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?
A. Database Administrator
B. Application Manager
C. Finance Manager
D. Privacy Officer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 370
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

A. Wi-Fi Protected Access 2 (WPA2) Enterprise
B. Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK)
C. Temporal Key Integrity Protocol (TKIP)
D. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
Answer: (SHOW ANSWER)

NEW QUESTION: 371
What should happen when an emergency change to a system must be performed?
A. Testing and approvals must be performed quickly.
B. The change must be given priority at the next meeting of the change control board.
C. The change is performed and a notation is made in the system log.
D. The change must be performed immediately and then submitted to the change board.
Answer: (SHOW ANSWER)

NEW QUESTION: 372
What does an organization FIRST review to assure compliance with privacy requirements?
A. Best practices
B. Business objectives
C. Employee's compliance to policies and standards
D. Legal and regulatory mandates
Answer: (SHOW ANSWER)

NEW QUESTION: 373
How can lessons learned from business continuity training and actual recovery incidents BEST be used?
A. As indicators of a need for policy

B. As alternative options for awareness and training
C. As a means for improvement
D. As business function gap indicators
Answer: C (LEAVE A REPLY)