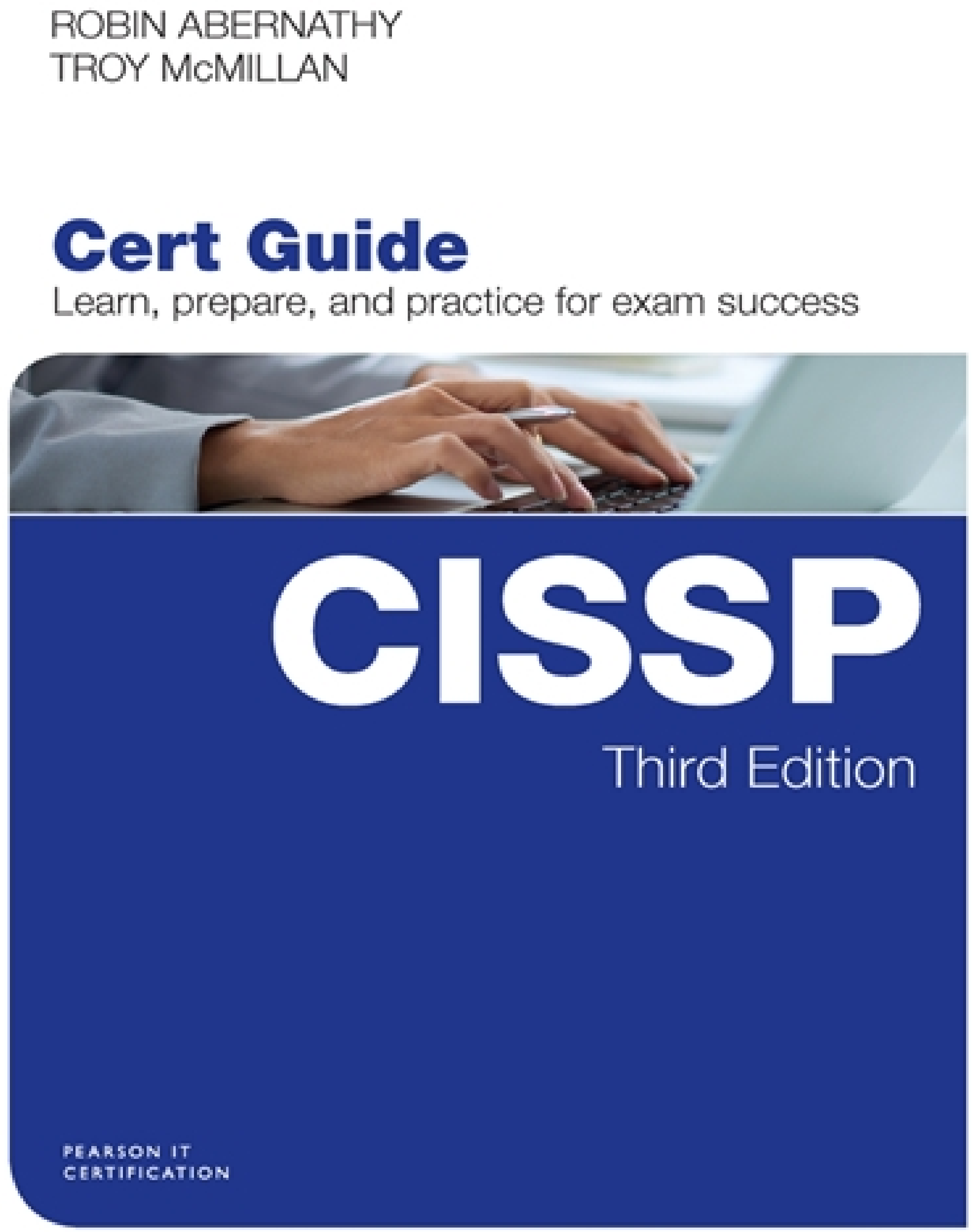
Test Bank for CISSP Cert Guide 3rd Edition by Abernathy

CLICK HERE TO ACCESS COMPLETE Test Bank



Test Bank

Question ID: CISSP-2018-CQ-01-001

Question: Which security principle is the opposite of disclosure?

A: integrity
B: availability
C: confidentiality
D: authorization

Answer(s): C

Explanation: The opposite of disclosure is confidentiality. The opposite of corruption is integrity. The opposite of destruction is availability. The opposite of disapproval is authorization.

Question ID: CISSP-2018-CQ-01-002

Question: Which of the following controls is an administrative control?

A: security policy
B: CCTV
C: data backups
D: locks

Answer(s): A

Explanation: A security policy is an administrative control. CCTV and locks are physical controls. Data backups are a technical control.

Question ID: CISSP-2018-CQ-01-003

Question: What is a vulnerability?

A: the entity that carries out a threat
B: the exposure of an organizational asset to losses
C: an absence or a weakness of a countermeasure that is in place
D: a control that reduces risk

Answer(s): C

Explanation: A vulnerability is an absence or a weakness of a countermeasure that is in place. A threat occurs when a vulnerability is identified or exploited. A threat agent is the entity that carries out a threat. Exposure occurs when an organizational asset is exposed to losses. A countermeasure or safeguard is a control that reduces risk.

Question ID: CISSP-2018-CQ-01-004

Question: Which framework uses the six communication questions (What, Where, When, Why, Who, and How) that intersect with six layers (operational, component, physical, logical, conceptual, and contextual)?

A: Six Sigma
B: SABSA
C: ITIL
D: ISO/IEC 27000 series

Answer(s): B

Explanation: SABSA uses the six communication questions (What, Where, When, Why, Who, and How) that intersect with six layers (operational, component, physical, logical, conceptual, and contextual). Six Sigma is a process improvement standard that includes two project methodologies that were inspired by Deming's Plan-Do-Check-Act cycle. ITIL is a process management development standard that has five core publications: ITIL Service Strategy, ITIL Service Design, ITIL Service Transition, ITIL Service Operation, and ITIL Continual Service Improvement. The ISO/IEC 27000 Series includes a list of standards, each of which addresses a particular aspect of information security management.

Question ID: CISSP-2018-CQ-01-005

Question: Which group of threat agents includes hardware and software failure, malicious code, and new technologies?

A: human
B: natural
C: environmental
D: technical

Answer(s): D

Explanation: Technical threat agents include hardware and software failure, malicious code, and new technologies. Human threat agents include both malicious and non-malicious insiders and outsiders, terrorists, spies, and terminated personnel. Natural threat agents include floods, fires, tornadoes, hurricanes, earthquakes, or other natural disaster or weather event. Environmental threat agents include power and other utility failure, traffic issues, biological warfare, and hazardous material issues (such as spillage).

Question ID: CISSP-2018-CQ-01-006

Question: Which term indicates the monetary impact of each threat occurrence?

A: ARO
B: ALE
C: EF

D: SLE

Answer(s): D

Explanation: SLE indicates the monetary impact of each threat occurrence. ARO is the estimate of how often a given threat might occur annually. ALE is the expected risk factor of an annual threat event. EF is the percent value or functionality of an asset that will be lost when a threat event occurs.

Question ID: CISSP-2018-CQ-01-007

Question: What is risk avoidance?

A: risk that is left over after safeguards have been implemented
B: terminating the activity that causes a risk or choosing an alternative that is not as risky
C: passing the risk on to a third party
D: defining the acceptable risk level the organization can tolerate and reducing the risk to that level

Answer(s): B

Explanation: Risk avoidance is terminating the activity that causes a risk or choosing an alternative that is not as risky. Residual risk is risk that is left over after safeguards have been implemented. Risk transfer is passing the risk on to a third party. Risk mitigation is defining the acceptable risk level the organization can tolerate and reducing the risk to that level.

Question ID: CISSP-2018-CQ-01-008

Question: Which security policies provide instruction on acceptable and unacceptable activities?

A: informative security policies
B: regulatory security policies
C: system-specific security policies
D: advisory security policies

Answer(s): D

Explanation: Advisory security policies provide instruction on acceptable and unacceptable activities. Informative security policies provide information on certain topics and act as an educational tool. Regulatory security policies address specific industry regulations, including mandatory standards. System-specific security policies address security for a specific computer, network, technology, or application.

Question ID: CISSP-2018-CQ-01-009

Question: Which organization role determines the classification level of the information to protect the data for which he is responsible?

A: data owner
B: data custodian
C: security administrator
D: security analyst

Answer(s): A

Explanation: The data owner determines the classification level of the information to protect the data for which he or she is responsible. The data custodian implements the information classification and controls after they are determined. The security administrator maintains security devices and software. The security analyst analyzes the security needs of the organizations and develops the internal information security governance documents.

Question ID: CISSP-2018-CQ-01-010

Question: Which type of crime occurs when a computer is used as a tool to help commit a crime?

A: computer-assisted crime
B: incidental computer crime
C: computer-targeted crime
D: computer prevalence crime

Answer(s): A

Explanation: A computer-assisted crime occurs when a computer is used as a tool to help commit a crime. An incidental computer crime occurs when a computer is involved in a computer crime without being the victim of the attack or the attacker. A computer-targeted crime occurs when a computer is the victim of an attack in which the sole purpose is to harm the computer and its owner. A computer prevalence crime occurs due to the fact that computers are so widely used in today's world.

Question ID: CISSP-2018-CQ-01-011

Question: Which access control type reduces the effect of an attack or another undesirable event?

A: compensative control
B: preventive control
C: detective control
D: corrective control

Answer(s): D

Explanation: A corrective control reduces the effect of an attack or other undesirable event. A compensative control substitutes for a primary access control and mainly acts as mitigation to risks. A preventive control prevents an attack from occurring. A detective control detects an attack while it is occurring to alert appropriate personnel.

Question ID: CISSP-2018-CQ-01-012

Question: What is the first stage of the security program life cycle?

A: Plan and Organize
B: Implement
C: Operate and Maintain
D: Monitor and Evaluate

Answer(s): A

Explanation: The four stages of the security program life cycle, in order, are as follows:

1. Plan and Organization
2. Implement
3. Operate and Maintain
4. Monitor and Evaluate

Question ID: CISSP-2018-CQ-01-013

Question: Which of the following frameworks is a two-dimensional model that intersects communication interrogatives (What, Why, Where, and so on) with various viewpoints (Planner, Owner, Designer, and so on)?

A: SABSA
B: Zachman framework
C: TOGAF
D: ITIL

Answer(s): B

Explanation: The Zachman framework is a two-dimensional model that intersects communication interrogatives (What, Why, Where, and so on) with various viewpoints (Planner, Owner, Designer, and so on). It is designed to help optimize communication between the various viewpoints during the creation of the security architecture.

Question ID: CISSP-2018-CQ-01-014

Question: Which management officer implements and manages all aspects of security, including risk analysis, security policies and procedures, training, and emerging technologies?

A: CPO
B: CFO
C: CSO
D: CIO

Answer(s): C

Explanation: The chief security officer (CSO) is the officer that leads any security effort and reports directly to the chief executive officer (CEO). The chief privacy officer (CPO) is the officer responsible for private information and usually reports directly to the CIO. The chief financial officer (CFO) is the officer responsible for all financial aspects of an organization. The CFO reports directly to the CEO and must also provide financial data for the shareholders and government entities. The chief information officer (CIO) is the officer responsible for all information systems and technology used in the organization and reports directly to the CEO or CFO.

Question ID: CISSP-2018-CQ-01-015

Question: Which of the following do organizations have employees sign in order to protect trade secrets?

A: trademark
B: patent
C: DRM
D: NDA

Answer(s): D

Explanation: Most organizations that have trade secrets attempt to protect these secrets using non-disclosure agreements (NDAs). These NDAs must be signed by any entity that has access to information that is part of the trade secret. A trademark is an intellectual property type that ensures that the symbol, sound, or expression that identifies a product or an organization is protected from being used by another. A patent is an intellectual property type that covers an invention described in a patent application and is granted to an individual or company. Digital rights management (DRM) is used by hardware manufacturers, publishers, copyright holders, and individuals to control the use of digital content. This often also involves device controls.

Question ID: CISSP-2018-CQ-01-016

Question: Which type of access control type is an acceptable use policy (AUP) most likely considered?

A: corrective
B: detective
C: compensative
D: directive

Answer(s): D

Explanation: The most popular directive control is an acceptable use policy (AUP) that lists proper (and often examples of improper) procedures and behaviors that personnel must follow. Corrective controls are in place to reduce the effect of an attack or other undesirable event. Examples of corrective controls include installing fire extinguishers and implementing new firewall rules. Detective controls are in place to detect an attack while it is occurring to alert appropriate personnel. Examples of detective controls include motion detectors, IDSs, or guards. Compensative controls are in place to substitute for a primary access control and mainly act as a mitigation to risks. Examples of compensative controls include requiring two authorized signatures to release sensitive or confidential information and requiring two keys owned by different personnel to open a safety deposit box.

Question ID: CISSP-2018-CQ-01-017

Question: What is the legal term used to describe an organization taking all reasonable measures to prevent security breaches and also taking steps to mitigate damages caused by successful breaches?

A: due care
B: due diligence
C: default stance
D: qualitative risk analysis

Answer(s): A

Explanation: Due care is a legal term that is used when an organization took all reasonable measures to prevent security breaches and also took steps to mitigate damages caused by successful breaches. Due diligence is a legal term that is used when an organization investigated all vulnerabilities. The default stance is the default security posture used by the organization. An allow-by-default stance permits access to any data unless a need exists to restrict access. A deny-by-default stance is much stricter because it denies any access that is not explicitly permitted. Qualitative risk analysis is method of analyzing risk whereby intuition, experience, and best practice techniques are used to determine risk.

Question ID: CISSP-2018-CQ-01-018

Question: Which threat modeling perspective profiles malicious characteristics, skills, and motivation to exploit vulnerabilities?

A: application-centric
B: asset-centric
C: attacker-centric
D: hostile-centric

Answer(s): C

Explanation: Attacker-centric threat modeling profiles an attacker's characteristics, skills, and motivation to exploit vulnerabilities. Application-centric threat modeling uses application architecture diagrams to analyze threats. Asset-centric threat modeling uses attack trees, attack graphs, or displaying patterns to determine how an asset can be attacked. Hostile describes one of two threat actor categories: non-hostile and hostile.

Question ID: CISSP-2018-CQ-01-019

Question: Which of the following is NOT a consideration for security professionals during mergers and acquisitions?

A: new data types
B: new technology types
C: cost of the merger or acquisition
D: the other organization's security awareness training program

Answer(s): C

Explanation: A security professional should not be concerned with the cost of a merger or an acquisition. A security professional should only be concerned with issues that affect security and leave financial issues to financial officers.

Question ID: CISSP-2018-CQ-01-020

Question: What is the first step of CRAMM?

A: identify threats and vulnerabilities
B: identify and value assets
C: identify countermeasures
D: prioritize countermeasures

Answer(s): B

Explanation: CRAMM review includes three steps:

1. Identify and value assets.
2. Identify threats and vulnerabilities and calculate risks.
3. Identify and prioritize countermeasures.

Question ID: CISSP-2018-CQ-02-001

Question: What is the highest military security level?

A: Confidential

B: Top Secret
C: Private
D: Sensitive

Answer(s): B

Explanation: Military and governmental entities classify data using five main classification levels, listed from highest sensitivity level to lowest:

1. Top Secret
2. Secret
3. Confidential
4. Sensitive but unclassified
5. Unclassified

Question ID: CISSP-2018-CQ-02-002

Question: Which of the following is also called disk striping?

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

Answer(s): A

Explanation: RAID 0, also called disk striping, writes the data across multiple drives, but although it improves performance, it does not provide fault tolerance.

Question ID: CISSP-2018-CQ-02-003

Question: Which of the following is also called disk mirroring?

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

Answer(s): B

Explanation: RAID 1, also called disk mirroring, uses two disks and writes a copy of the data to both disks, providing fault tolerance in the case of a single drive failure.

Question ID: CISSP-2018-CQ-02-004

Question: Which of the following is composed of high-capacity storage devices that are connected by a high-speed private (separate from the LAN) network using storage-specific switches?

A: HSM
B: SAN
C: NAS
D: RAID

Answer(s): B

Explanation: Storage-area networks (SANs) are composed of high-capacity storage devices that are connected by a high-speed private (separate from the LAN) network using storage specific switches.

Question ID: CISSP-2018-CQ-02-005

Question: Who is responsible for deciding which users have access to data?

A: business owner
B: system owner
C: data owner
D: data custodian

Answer(s): C

Explanation: The data owner is responsible for deciding which users have access to data.

Question ID: CISSP-2018-CQ-02-006

Question: Which term is used for the fitness of data for use?

A: data sensitivity
B: data criticality
C: data quality
D: data classification

Answer(s): C

Explanation: Data quality is the fitness of data for use.

Question ID: CISSP-2018-CQ-02-007

Question: What is the highest level of classification for commercial systems?

A: public
B: sensitive

C: private
D: confidential

Answer(s): D

Explanation: Commercial systems usually use the following classifications, from highest to lowest:

1. Confidential
2. Private
3. Sensitive
4. Public

Question ID: CISSP-2018-CQ-02-008

Question: What is the first phase of the information life cycle?

A: maintain
B: use
C: distribute
D: create/receive

Answer(s): D

Explanation: The phases of the information life cycle are as follows:

1. Create/receive
2. Distribute
3. Use
4. Maintain
5. Dispose/store

Question ID: CISSP-2018-CQ-02-009

Question: Which organizational role owns a system and must work with other users to ensure that data is secure?

A: business owner
B: data custodian
C: data owner
D: system owner

Answer(s): D

Explanation: The system owner owns a system and must work with other users to ensure that data is secure.

Question ID: CISSP-2018-CQ-02-010

Question: What is the last phase of the information life cycle?

A: distribute
B: maintain
C: dispose/store
D: use

Answer(s): C

Explanation: The phases of the information life cycle are as follows:

1. Create/receive
2. Distribute
3. Use
4. Maintain
5. Dispose/store

Question ID: CISSP-2018-CQ-03-001

Question: Which of the following is provided if data cannot be read?

A: integrity
B: confidentiality
C: availability
D: defense in depth

Answer(s): B

Explanation: Confidentiality is provided if the data cannot be read. This can be provided either through access controls and encryption for data as it exists on a hard drive or through encryption as the data is in transit.

Question ID: CISSP-2018-CQ-03-002

Question: In a distributed environment, which of the following is software that ties the client and server software together?

A: embedded systems
B: mobile code
C: virtual computing
D: middleware

Answer(s): D

Explanation: In a distributed environment, middleware is software that ties the client and server software together. It is neither a part of the operating system nor a part of the server software. It is the code that lies between the operating system and applications on each side of a distributed computing system in a network.

Question ID: CISSP-2018-CQ-03-003

Question: Which of the following comprises the components (hardware, firmware, and/or software) that are trusted to enforce the security policy of the system?

A: security perimeter
B: reference monitor
C: Trusted Computer Base (TCB)
D: security kernel

Answer(s): C

Explanation: The TCB comprises the components (hardware, firmware, and/or software) that are trusted to enforce the security policy of the system and that if compromised jeopardize the security properties of the entire system.

Question ID: CISSP-2018-CQ-03-004

Question: Which process converts plaintext into ciphertext?

A: hashing
B: decryption
C: encryption
D: digital signature

Answer(s): C

Explanation: Encryption converts plaintext into ciphertext. Hashing reduces a message to a hash value. Decryption converts ciphertext into plaintext. A digital signature is an object that provides sender authentication and message integrity by including a digital signature with the original message.

Question ID: CISSP-2018-CQ-03-005

Question: Which type of cipher is the Caesar cipher?

A: polyalphabetic substitution
B: mono-alphabetic substitution
C: polyalphabetic transposition
D: mono-alphabetic transposition

Answer(s): B

Explanation: The Caesar cipher is a mono-alphabetic substitution cipher. The Vigenere substitution is a polyalphabetic substitution.

Question ID: CISSP-2018-CQ-03-006

Question: What is the most secure encryption scheme?

A: concealment cipher
B: symmetric algorithm
C: one-time pad
D: asymmetric algorithm

Answer(s): C

Explanation: A one-time pad is the most secure encryption scheme because it is used only once.

Question ID: CISSP-2018-CQ-03-007

Question: Which 3DES implementation encrypts each block of data three times, each time with a different key?

A: 3DES-EDE3
B: 3DES-EEE3
C: 3DES-EDE2
D: 3DES-EEE2

Answer(s): B

Explanation: The 3DES-EEE3 implementation encrypts each block of data three times, each time with a different key. The 3DES-EDE3 implementation encrypts each block of data with the first key, decrypts each block with the second key, and encrypts each block with the third key. The 3DES-EDE2 implementation encrypts each block of data with the first key, decrypts each block with the second key, and then encrypts each block with the first key. The 3DES-EEE2 implementation encrypts each block of data with the first key, encrypts each block with the second key, and then encrypts each block with the third key.

Question ID: CISSP-2018-CQ-03-008

Question: Which of the following is NOT a hash function?

A: ECC
B: MD6
C: SHA-2

D: RIPEMD-160

Answer(s): A

Explanation: ECC is NOT a hash function. It is an asymmetric algorithm. All the other options are hash functions.

Question ID: CISSP-2018-CQ-03-009

Question: Which of the following is an example of preventing an internal threat?

A: a door lock system on a server room
B: an electric fence surrounding a facility
C: armed guards outside a facility
D: parking lot cameras

Answer(s): A

Explanation: An electric fence surrounding a facility is designed to prevent access to the building by those who should not have any access (an external threat), whereas a door lock system on the server room that requires a swipe of the employee card is designed to prevent access by those who are already in the building (an internal threat).

Question ID: CISSP-2018-CQ-03-010

Question: Which of the following is NOT one of the three main strategies that guide CPTED?

A: Natural Access Control
B: Natural Surveillance Reinforcement
C: Natural Territorials Reinforcement
D: Natural Surveillance

Answer(s): B

Explanation: The three strategies are natural access control, natural territorials reinforcement, and natural surveillance.

Question ID: CISSP-2018-CQ-03-011

Question: What occurs when different encryption keys generate the same ciphertext from the same plaintext message?

A: key clustering
B: cryptanalysis
C: keyspace
D: confusion

Answer(s): A

Explanation: Key clustering occurs when different encryption keys generate the same ciphertext from the same plaintext message. Cryptanalysis is the science of decrypting ciphertext without prior knowledge of the key or cryptosystem used. A keyspace is all the possible key values when using a particular algorithm or other security measure. Confusion is the process of changing a key value during each round of encryption.

Question ID: CISSP-2018-CQ-03-012

Question: Which encryption system uses a private or secret key that must remain secret between the two parties?

A: running key cipher
B: concealment cipher
C: asymmetric algorithm
D: symmetric algorithm

Answer(s): D

Explanation: A symmetric algorithm uses a private or secret key that must remain secret between the two parties. A running key cipher uses a physical component, usually a book, to provide the polyalphabetic characters. A concealment cipher occurs when plaintext is interspersed somewhere within other written material. An asymmetric algorithm uses both a public key and a private or secret key.

Question ID: CISSP-2018-CQ-03-013

Question: Which of the following is an asymmetric algorithm?

A: IDEA
B: Twofish
C: RC6
D: RSA

Answer(s): D

Explanation: RSA is an asymmetric algorithm. All the other algorithms are symmetric algorithms.

Question ID: CISSP-2018-CQ-03-014

Question: Which PKI component contains a list of all the certificates that have been revoked?

A: CA

B: RA
C: CRL
D: OCSP

Answer(s): C

Explanation: A CRL contains a list of all the certificates that have been revoked. A CA is the entity that creates and signs digital certificates, maintains the certificates, and revokes them when necessary. An RA verifies the requestor's identity, registers the requestor, and passes the request to the CA. OCSP is an Internet protocol that obtains the revocation status of an X.509 digital certificate.

Question ID: CISSP-2018-CQ-03-015

Question: Which attack executed against a cryptographic algorithm uses all possible keys until a key is discovered that successfully decrypts the ciphertext?

A: frequency analysis
B: reverse engineering
C: ciphertext-only attack
D: brute force

Answer(s): D

Explanation: A brute-force attack executed against a cryptographic algorithm uses all possible keys until a key is discovered that successfully decrypts the ciphertext. A frequency analysis attack relies on the fact that substitution and transposition ciphers will result in repeated patterns in ciphertext. A reverse engineering attack occurs when an attacker purchases a particular cryptographic product to attempt to reverse engineer the product to discover confidential information about the cryptographic algorithm used. A ciphertext-only attack uses several encrypted messages (ciphertext) to figure out the key used in the encryption process.

Question ID: CISSP-2018-CQ-03-016

Question: In ISO/IEC 15288:2018, which process category includes acquisition and supply?

A: Technical management processes
B: Technical processes
C: Agreement processes
D: Organizational project-enabling processes

Answer(s): C

Explanation: ISO/IEC 15288:2018 establishes four categories of processes:

- Agreement processes, including acquisition and supply
- Organizational project-enabling processes, including infrastructure management, quality

management, and knowledge management
- Technical management processes, including project planning, risk management, configuration management, and quality assurance
- Technical processes, including system requirements definition, system analysis, implementation, integration, operation, maintenance, and disposal

Question ID: CISSP-2018-CQ-03-017

Question: Which of the following is NOT a principle in the risk-based category of NIST 800-27 Rev A?

A: Assume that external systems are insecure.
B: Eliminate risk.
C: Protect information while being processed, in transit, and in storage.
D: Protect against all likely classes of attacks.

Answer(s): B

Explanation: NIST 800-27 Rev A does NOT require that risk be eliminated. These are the risk-based principles in NIST 800-27 Rev A:
- Reduce risk to an acceptable level.
- Assume that external systems are insecure.
- Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
- Implement tailored system security measures to meet organizational security goals.
- Protect information while being processed, in transit, and in storage.
- Consider custom products to achieve adequate security.
- Protect against all likely classes of attacks.

Question ID: CISSP-2018-CQ-03-018

Question: Which statement is true of dedicated security mode?

A: It employs a single classification level.
B: All users have the same security clearance, but they do not all possess a need-to-know clearance for all the information in the system.
C: All users must possess the highest security clearance, but they must also have valid need-to-know clearance, a signed NDA, and formal approval for all information to which they have access.
D: Systems allow two or more classification levels of information to be processed at the same time.

Answer(s): A

Explanation: Dedicated security mode employs a single classification level.

Question ID: CISSP-2018-CQ-03-019

Question: What is the first step in ISO/IEC 27001:2013?

A: Identify the requirements.
B: Perform risk assessment and risk treatment.
C: Maintain and monitor the ISMS.
D: Obtain management support.

Answer(s): D

Explanation: The first step in ISO/IEC 27001:2013 is to obtain management support.

Question ID: CISSP-2018-CQ-03-020

Question: Which two processor states are supported by most processors?

A: supervisor state and problem state
B: supervisor state and kernel state
C: problem state and user state
D: supervisor state and elevated state

Answer(s): A

Explanation: Two processor states are supported by most processors: supervisor state (or kernel mode) and problem state (or user mode).

Question ID: CISSP-2018-CQ-03-021

Question: When supporting a BYOD initiative, from which group do you probably have most to fear?

A: hacktivists
B: careless users
C: software vendors
D: mobile device vendors

Answer(s): B

Explanation: As a security professional, when supporting a BYOD initiative, you should take into consideration that you probably have more to fear from the carelessness of the users than you do from hackers.

Question ID: CISSP-2018-CQ-03-022

Question: Which term for applies to embedded devices that bring with them security concerns because engineers that design these devices do not always worry about security?

A: BYOD
B: NDA
C: IoT
D: ITSEC

Answer(s): C

Explanation: Internet of Things (IoT) is the term is used for embedded devices and their security concerns because engineers that design these devices do not always worry about security.

Question ID: CISSP-2018-CQ-03-023

Question: Which option best describes the primary concern of NIST SP 800-57?

A: asymmetric encryption
B: symmetric encryption
C: message integrity
D: key management

Answer(s): D

Explanation: Key management is the primary concern of NIST SP 800-57.

Question ID: CISSP-2018-CQ-03-024

Question: Which of the following key types requires only integrity security protection?

A: public signature verification key
B: private signature key
C: symmetric authentication key
D: private authentication key

Answer(s): A

Explanation: Public signature verification keys require only integrity security protection.

Question ID: CISSP-2018-CQ-03-025

Question: What is the final phase of the cryptographic key management life cycle, according to NIST SP 800-57?

A: operational phase
B: destroyed phase
C: pre-operational phase
D: post-operational phase

Answer(s): B

Explanation: The destroyed phase is the final phase of the cryptographic key management life cycle, according to NIST SP 800-57.

Question ID: CISSP-2018-CQ-04-001

Question: At which layer of the OSI model does the encapsulation process begin?

A: Transport
B: Application
C: Physical
D: Session

Answer(s): B

Explanation: The Application layer (layer 7) is where the encapsulation process begins. This layer receives the raw data from the application in use and provides services such as file transfer and message exchange to the application (and thus the user).

Question ID: CISSP-2018-CQ-04-002

Question: Which two layers of the OSI model are represented by the Link layer of the TCP/IP model? (Choose two.)

A: Data Link
B: Physical
C: Session
D: Application
E: Presentation

Answer(s): A,B

Explanation: The Link layer of the TCP/IP model provides the services provided by both the Data Link and the Physical layers in the OSI model.

Question ID: CISSP-2018-CQ-04-003

Question: Which of the following represents the range of port numbers that are referred to as "well-known" port numbers?

A: 49152-65535
B: 0-1023
C: 1024-49151
D: all above 500

Answer(s): B

Explanation: The port numbers in the range 0 to 1023 are the well-known ports, or system ports. They are assigned by the IETF for standards-track protocols, as per RFC 6335.

Question ID: CISSP-2018-CQ-04-004

Question: What is the port number for HTTP?

A: 23
B: 443
C: 80
D: 110

Answer(s): C

Explanation: The listed ports numbers are as follows:

23 - Telnet

443 - HTTPS

80 - HTTP

110 - POP3

Question ID: CISSP-2018-CQ-04-005

Question: What protocol in the TCP/IP suite resolves IP addresses to MAC addresses?

A: ARP
B: TCP
C: IP
D: ICMP

Answer(s): A

Explanation: Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses.

Question ID: CISSP-2018-CQ-04-006

Question: How many bits are contained in an IPv4 address?

A: 128
B: 48
C: 32
D: 64

Answer(s): C

Explanation: IPv4 addresses are 32 bits in length and can be represented in either binary or in dotted decimal format. IPv6 addresses are 128 bits in length and are composed of hexadecimal characters.

Question ID: CISSP-2018-CQ-04-007

Question: Which of the following is a Class C address?

A: 172.16.5.6
B: 192.168.5.54
C: 10.6.5.8
D: 224.6.6.6

Answer(s): B

Explanation: The IP Class C range of addresses is from 192.0.0.0 to 223.255.255.255.

Question ID: CISSP-2018-CQ-04-008

Question: Which of the following is a valid private IP address?

A: 10.2.6.6
B: 172.15.6.6
C: 191.6.6.6
D: 223.54.5.5

Answer(s): A

Explanation: Valid private IP address ranges are:

Class	**Range**
Class A	10.0.0.0-10.255.255.255

Class B	172.16.0.0-172.31.255.255
Class C	192.168.0.0-192.168.255.255

Question ID: CISSP-2018-CQ-04-009

Question: Which service converts private IP addresses to public IP addresses?

A: DHCP
B: DNS
C: NAT
D: WEP

Answer(s): C

Explanation: Network address translation (NAT) is a service that can be supplied by a router or by a server. The device that provides the service stands between the local LAN and the Internet. When packets need to go to the Internet, the packets go through the NAT service first. The NAT service changes the private IP address to a public address that is routable on the Internet. When the response is returned from the Web, the NAT service receives it and translates the address back to the original private IP address and sends it back to the originator.

Question ID: CISSP-2018-CQ-04-010

Question: Which type of transmission uses stop and start bits?

A: asynchronous
B: unicast
C: multicast
D: synchronous

Answer(s): A

Explanation: With asynchronous transmission, the systems use start and stop bits to communicate when each byte is starting and stopping. This method also uses what are called parity bits to be used for the purpose of ensuring that each byte has not changed or been corrupted en route. This introduces additional overhead to the transmission.

Question ID: CISSP-2018-CQ-04-011

Question: Which protocol encapsulates Fibre Channel frames over Ethernet networks?

A: MPLS
B: FCoE
C: iSCSI
D: VoIP

Answer(s): B

Explanation: Fibre Channel over Ethernet (FCoE) encapsulates Fibre Channel frames over Ethernet networks.

Question ID: CISSP-2018-CQ-04-012

Question: Which protocol uses port 143?

A: RDP
B: AFP
C: IMAP
D: SSH

Answer(s): C

Explanation: IMAP uses port 143.

Question ID: CISSP-2018-CQ-04-013

Question: Which of the following best describes NFS?

A: a file-sharing protocol
B: a directory query protocol that is based on X.500
C: an Application layer protocol that is used to retrieve information from network devices
D: a client/server file-sharing protocol used in UNIX/Linux

Answer(s): D

Explanation: NFS is a client/server file-sharing protocol used in UNIX/Linux.

Question ID: CISSP-2018-CQ-04-014

Question: Which of the following is a multi-layer protocol that is used between components in process automation systems in electric and water companies?

A: DNP3
B: VoIP
C: WPA

D: WPA2

Answer(s): A

Explanation: DNP3 is a multi-layer protocol that is used between components in process automation systems in electric and water companies

Question ID: CISSP-2018-CQ-04-015

Question: Which wireless implementation includes MU MIMO?

A: 802.11a
B: 802.11ac
C: 802.11g
D: 802.11n

Answer(s): B

Explanation: 802.11ac includes MU MIMO.

Question ID: CISSP-2018-CQ-05-001

Question: Which of the following is NOT an example of a knowledge authentication factor?

A: password
B: mother's maiden name
C: city of birth
D: smart card

Answer(s): D

Explanation: Knowledge factors are something a person knows, including passwords, mother's maiden name, city of birth, and date of birth. Ownership factors are something a person has, including a smart card.

Question ID: CISSP-2018-CQ-05-002

Question: Which of the following statements about memory cards and smart cards is false?

A: A memory card is a swipe card that contains user authentication information.
B: Memory cards are also known as integrated circuit cards (ICCs).
C: Smart cards contain memory and an embedded chip.
D: Smart card systems are more reliable than memory card systems.

Answer(s): B

Explanation: Memory cards are NOT also known as integrated circuit cards (ICCs). Smart cards are also known as ICCs.

Question ID: CISSP-2018-CQ-05-003

Question: Which biometric method is most effective?

A: iris scan
B: retina scan
C: fingerprint
D: hand print

Answer(s): A

Explanation: Iris scans are considered more effective than retina scans, fingerprints, and hand prints.

Question ID: CISSP-2018-CQ-05-004

Question: What is a Type I error in a biometric system?

A: crossover error rate (CER)
B: false rejection rate (FRR)
C: false acceptance rate (FAR)
D: throughput rate

Answer(s): B

Explanation:

Question ID: CISSP-2018-CQ-05-005

Question: Which access control model is most often used by routers and firewalls to control access to networks?

A: discretionary access control
B: mandatory access control
C: role-based access control
D: rule-based access control

Answer(s): D

Explanation: Rule-based access control is most often used by routers and firewalls to control access to networks. The other three types of access control models are not usually implemented by routers and firewalls.

Question ID: CISSP-2018-CQ-05-006

Question: Which threat is NOT considered a social engineering threat?

A: phishing
B: pharming
C: DoS attack
D: dumpster diving

Answer(s): C

Explanation: A denial-of-service (DoS) attack is not considered a social engineering threat. The other three options are considered to be social engineering threats.

Question ID: CISSP-2018-CQ-05-007

Question: Which of the following statements best describes an IDaaS implementation?

A: Ensures that any instance of identification and authentication to a resource is managed properly.
B: Collects and verifies information about an individual to prove that the person who has a valid account is who he or she claims to be.
C: Provides a set of identity and access management functions to target systems on customers' premises and/or in the cloud.
D: It is an SAML standard that exchanges authentication and authorization data between organizations or security domains.

Answer(s): C

Explanation: An Identity as a Service (IDaaS) implementation provides a set of identity and access management functions to target systems on customers' premises and/or in the cloud. Session management ensures that any instance of identification and authentication to a resource is managed properly. A proof of identity process collects and verifies information about an individual to prove that the person who has a valid account is who he or she claims to be.

Question ID: CISSP-2018-CQ-05-008

Question: Which of the following is an example of multi-factor authentication?

A: username and password
B: username, retina scan, and smart card
C: retina scan and finger scan
D: smart card and security token

Answer(s): B

Explanation: Using username, retina scan, and a smart card is an example of multi-factor authentication. The username is something you know, the retina scan is something you are, and the smart card is something you have.

Question ID: CISSP-2018-CQ-05-009

Question: You decide to implement an access control policy that requires that users logon from certain workstations within your enterprise. Which type of authentication factor are you implementing?

A: knowledge factor
B: location factor
C: ownership factor
D: characteristic factor

Answer(s): B

Explanation: You are implementing location factors, which are based on where a person is located when logging in.

Question ID: CISSP-2018-CQ-05-010

Question: Which threat is considered a password threat?

A: buffer overflow
B: sniffing
C: spoofing
D: brute-force attack

Answer(s): D

Explanation: A brute-force attack is considered a password threat.

Question ID: CISSP-2018-CQ-05-011

Question: Which session management mechanisms are often used to manage desktop sessions?

A: screensavers and timeouts
B: FIPS 201.2 and NIST SP 800-79-2
C: Bollards and locks
D: KDC, TGT, and TGS

Answer(s): A

Explanation: Desktop sessions can be managed through screensavers, timeouts, logon, and schedule limitations. Federal Information Processing Standards (FIPS) Publication 201.2 and

NIST Special Publication 800-79-2 are documents that provide guidance on proof of identity. Physical access to facilities can be provided securely using locks, fencing, bollards, guards, and closed-circuit television (CCTV). In Kerberos, the key distribution center (KDC) issues a ticket-granting ticket (TGT) to the principal. The principal sends the TGT to the ticket-granting service (TGS) when the principal needs to connect to another entity.

Question ID: CISSP-2018-CQ-05-012

Question: Which of the following is a major disadvantage of implementing an SSO system?

A: Users are able to use stronger passwords.
B: Users need to remember the login credentials for a single system.
C: User and password administration are simplified.
D: If a user's credentials are compromised, attacker can access all resources.

Answer(s): D

Explanation: If a user's credentials are compromised in a single sign-on (SSO) environment, attackers have access to all resources to which the user has access. All other choices are advantages to implementing an SSO system.

Question ID: CISSP-2018-CQ-05-013

Question: Which type of attack is carried out from multiple locations using zombies and botnets?

A: TEMPEST
B: DDoS
C: Backdoor
D: Emanating

Answer(s): B

Explanation: A distributed DoS (DDoS) attack is a DoS attack that is carried out from multiple attack locations. Vulnerable devices are infected with software agents, called zombies. This turns the vulnerable devices into botnets, which then carry out the attack. Devices that meet TEMPEST standards implement an outer barrier or coating, called a Faraday cage or Faraday shield. A backdoor or trapdoor is a mechanism implemented in many devices or applications that gives the user who uses the backdoor unlimited access to the device or application. Emanations are electromagnetic signals that are emitted by an electronic device. Attackers can target certain devices or transmission mediums to eavesdrop on communication without having physical access to the device or medium.

Question ID: CISSP-2018-CQ-06-000

Question: Which monitoring method captures and analyzes every transaction of every