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

application or website user?

A: RUM
B: synthetic transaction monitoring
C: code review and testing
D: misuse case testing

Answer(s): A

Explanation: Real user monitoring (RUM) captures and analyzes every transaction of every application or website user.

Question ID: CISSP-2018-CQ-06-001

Question: For which of the following penetration tests does the testing team know an attack is coming but have limited knowledge of the network systems and devices and only publicly available information?

A: target test
B: physical test
C: blind test
D: double-blind test

Answer(s): C

Explanation: With a blind test, the testing team knows an attack is coming and has limited knowledge of the network systems and devices and publicly available information. A target test occurs when the testing team and the organization's security team are given maximum information about the network and the type of attack that will occur. A physical test is not a type of penetration test. It is a type of vulnerability assessment. A double-blind test is like a blind test except that the organization's security team does not know an attack is coming.

Question ID: CISSP-2018-CQ-06-002

Question: Which of the following is NOT a guideline according to NIST SP 800-92?

A: Organizations should establish policies and procedures for log management.
B: Organizations should create and maintain a log management infrastructure.
C: Organizations should prioritize log management appropriately throughout the organization.
D: Choose auditors with security experience.

Answer(s): D

Explanation: NIST SP 800-92 does not include any information regarding auditors. So the “Choose auditors with security experience” option is NOT a guidelines according to NIST SP 800-92.

Question ID: CISSP-2018-CQ-06-003

Question: According to NIST SP 800-92, which of the following are facets of log management infrastructure? (Choose all that apply.)

A: general functions (log parsing, event filtering, and event aggregation)
B: storage (log rotation, log archival, log reduction, log conversion, log normalization, log file integrity checking)
C: log analysis (event correlation, log viewing, log reporting)
D: log disposal (log clearing)

Answer(s): A,B,C,D

Explanation: According to NIST SP 800-92, log management functions should include general functions (log parsing, event filtering, and event aggregation), storage (log rotation, log archival, log reduction, log conversion, log normalization, log file integrity checking), log analysis (event correlation, log viewing, log reporting), and log disposal (log clearing.)

Question ID: CISSP-2018-CQ-06-004

Question: What are the two ways of collecting logs using security information and event management (SIEM) products, according to NIST SP 800-92?

A: passive and active
B: agentless and agent-based
C: push and pull
D: throughput and rate

Answer(s): B

Explanation: The two ways of collecting logs using security information and event management (SIEM) products, according to NIST SP 800-92, are agentless and agent-based.

Question ID: CISSP-2018-CQ-06-006

Question: Which type of testing is also known as negative testing?

A: RUM
B: synthetic transaction monitoring
C: code review and testing
D: misuse case testing

Answer(s): D

Explanation: Misuse case testing is also known as negative testing.

Question ID: CISSP-2018-CQ-06-007

Question: What is the first step of the information security continuous monitoring (ISCM) plan, according to NIST SP 800-137?

A: Establish an ISCM program.
B: Define the ISCM strategy.
C: Implement an ISCM program.
D: Analyze the data collected.

Answer(s): B

Explanation: The steps in an ISCM program, according to NIST SP 800-137, are:

1. Define an ISCM strategy.

2. Establish an ISCM program.

3. Implement an ISCM program.

4. Analyze the data collected, and report findings.

5. Respond to findings.

6. Review and update the monitoring program.

Question ID: CISSP-2018-CQ-06-008

Question: What is the second step of the information security continuous monitoring (ISCM) plan, according to NIST SP 800-137?

A: Establish an ISCM program.
B: Define the ISCM strategy.
C: Implement an ISCM program.
D: Analyze the data collected.

Answer(s): A

Explanation: The steps in an ISCM program, according to NIST SP 800-137, are:

1. Define an ISCM strategy.

2. Establish an ISCM program.

3. Implement an ISCM program.

4. Analyze the data collected, and report findings.

5. Respond to findings.

6. Review and update the monitoring program.

Question ID: CISSP-2018-CQ-06-009

Question: Which of the following is NOT a guideline for internal and third-party audits?

A: Choose auditors with security experience.
B: Define the ISCM strategy.
C: Implement an ISCM program.
D: Analyze the data collected.

Answer(s): C

Explanation: The following are guidelines for internal and third-party audits:

- At minimum, perform annual audits to establish a security baseline.
- Determine your organization's objectives for the audit and share them with the auditors.
- Set the ground rules for the audit, including the dates/times of the audit, before the audit starts.
- Choose auditors who have security experience.
- Involve business unit managers early in the process.
- Ensure that auditors rely on experience, not just checklists.
- Ensure that the auditor's report reflects risks that the organization has identified.
- Ensure that the audit is conducted properly.
- Ensure that the audit covers all systems and all policies and procedures.
- Examine the report when the audit is complete.

Question ID: CISSP-2018-CQ-06-010

Question: Which SOC report should be shared with the general public?

A: SOC 1, Type 1
B: SOC 1, Type 2
C: SOC 2
D: SOC 3

Answer(s): D

Explanation: SOC 3 is the only SOC report that should be shared with the general public.

Question ID: CISSP-2018-CQ-07-001

Question: What is the first step of the incident response process?

A: Respond to the incident.
B: Detect the incident.
C: Report the incident.
D: Recover from the incident.

Answer(s): B

Explanation: The steps of the incident response process are as follows:

1. Detect the incident.

2. Respond to the incident.

3. Report the incident to the appropriate personnel.

4. Recover from the incident.

5. Remediate all components affected by the incident to ensure that all traces of the incident have been removed.

6. Review the incident and document all findings.

Question ID: CISSP-2018-CQ-07-002

Question: What is the second step of the forensic investigations process?

A: identification
B: collection
C: preservation
D: examination

Answer(s): C

Explanation: The steps of the forensic investigation process are as follows:

1. Identification

2. Preservation

3. Collection

4. Examination
5. Analysis
6. Presentation
7. Decision

Question ID: CISSP-2018-CQ-07-003

Question: Which of the following is NOT one of the five rules of evidence?

A: Be accurate.
B: Be complete.
C: Be admissible.
D: Be volatile.

Answer(s): D

Explanation: The five rules of evidence are as follows:

- Be authentic.
- Be accurate.
- Be complete.
- Be convincing.
- Be admissible.

Question ID: CISSP-2018-CQ-07-004

Question: Which of the following refers to allowing users access only to the resources required to do their jobs?

A: job rotation
B: separation of duties
C: need to know/least privilege
D: mandatory vacation

Answer(s): C

Explanation: When allowing access to resources and assigning rights to perform operations, the concept of least privilege (also called need to know) should always be applied. In the context of resource access, this means the default level of access should be no access. Give users access only to resources required to do their jobs, and that access should require manual implementation after the requirement is verified by a supervisor.

Question ID: CISSP-2018-CQ-07-005

Question: Which of the following is an example of an intangible asset?

A: disc drive
B: recipe
C: people
D: server

Answer(s): B

Explanation: In many cases, some of the most valuable assets for a company are intangible ones, such as secret recipes, formulas, and trade secrets.

Question ID: CISSP-2018-CQ-07-006

Question: Which of the following is not a step in incident response management?

A: detect
B: respond
C: monitor
D: report

Answer(s): C

Explanation: The steps in incident response management are:

1. Detect
2. Respond
3. Report
4. Recover
5. Remediate
6. Review

Question ID: CISSP-2018-CQ-07-007

Question: Which of the following is NOT a backup type?

A: full

B: incremental
C: grandfather/father/son
D: transaction log

Answer(s): C

Explanation: Grandfather/father/son is not a backup type; it is a backup rotation scheme.

Question ID: CISSP-2018-CQ-07-008

Question: Which term is used for a leased facility that contains all the resources needed for full operation?

A: cold site
B: hot site
C: warm site
D: tertiary site

Answer(s): B

Explanation: A hot site is a leased facility that contains all the resources needed for full operation.

Question ID: CISSP-2018-CQ-07-009

Question: Which electronic backup type stores data on optical discs and uses robotics to load and unload the optical disks as needed?

A: optical jukebox
B: hierarchical storage management
C: tape vaulting
D: replication

Answer(s): A

Explanation: An optical jukebox stores data on optical discs and uses robotics to load and unload the optical discs as needed.

Question ID: CISSP-2018-CQ-07-010

Question: What is failsoft?

A: the capacity of a system to switch over to a backup system if a failure in the primary system occurs
B: the capability of a system to terminate non-critical processes when a failure occurs
C: a software product that provides load-balancing services

D: high-capacity storage devices that are connected by a high-speed private network using storage-specific switches

Answer(s): B

Explanation: Failsoft is the capability of a system to terminate non-critical processes when a failure occurs.

Question ID: CISSP-2018-CQ-07-011

Question: What investigation type specifically refers to litigation or government investigations that deal with the exchange of information in electronic format as part of the discovery process?

A: data loss prevention (DLP)
B: regulatory
C: eDiscovery
D: operations

Answer(s): C

Explanation: Electronic discovery (eDiscovery) refers to litigation or government investigations that deal with the exchange of information in electronic format as part of the discovery process. It involves electronically stored information (ESI) and includes emails, documents, presentations, databases, voicemail, audio and video files, social media, and websites. Data loss prevention (DLP) software attempts to prevent data leakage. It does this by maintaining awareness of actions that can and cannot be taken with respect to a document. A regulatory investigation occurs when a regulatory body investigates an organization for a regulatory infraction. Operations investigations involve any investigations that do not result in any criminal, civil, or regulatory issue. In most cases, this type of investigation is completed to determine the root cause so that steps can be taken to prevent this incident in the future.

Question ID: CISSP-2018-CQ-07-012

Question: An organization's firewall is monitoring the outbound flow of information from one network to another. What specific type of monitoring is this?

A: egress monitoring
B: continuous monitoring
C: CMaaS
D: resource provisioning

Answer(s): A

Explanation: Egress monitoring occurs when an organization monitors the outbound flow of information from one network to another. The most popular form of egress monitoring is carried out using firewalls that monitor and control outbound traffic. Continuous monitoring and

Continuous Monitoring as a Service (CMaaS) are not specific enough to answer this question. Any logging and monitoring activities should be part of an organizational continuous monitoring program. The continuous monitoring program must be designed to meet the needs of the organization and implemented correctly to ensure that the organization's critical infrastructure is guarded. Organizations may want to look into CMaaS solutions deployed by cloud service providers. Resource provisioning is the process in security operations that ensures that the organization only deploys the assets that it currently needs.

Question ID: CISSP-2018-CQ-07-013

Question: Which of the following are considered virtual assets? (Choose all that apply.)

A: software-defined networks
B: virtual storage-area networks
C: guest OSs deployed on VMs
D: virtual routers

Answer(s): A,B,C,D

Explanation: Virtual assets include software-defined networks, virtual storage-area networks (VSANs), guest operating systems deployed on virtual machines (VMs), and virtual routers. As with physical assets, the deployment and decommissioning of virtual assets should be tightly controlled as part of configuration management because virtual assets, like physical assets, can be compromised.

Question ID: CISSP-2018-CQ-07-014

Question: Which of the following describes the ability of a system, device, or data center to recover quickly and continue operating after an equipment failure, power outage, or other disruption?

A: quality of service (QoS)
B: recovery time objective (RTO)
C: recovery point objective (RPO)
D: system resilience

Answer(s): D

Explanation: System resilience is the ability of a system, device, or data center to recover quickly and continue operating after an equipment failure, power outage, or other disruption. It involves the use of redundant components or facilities. Quality of service (QoS) is a technology that manages network resources to ensure a predefined level of service. It assigns traffic priorities to the different types of traffic on a network. A recovery time objective (RTO) stipulates the amount of time an organization needs to recover from a disaster, and a recovery point objective (RPO) stipulates the amount of data an organization can lose when a disaster occurs.

Question ID: CISSP-2018-CQ-07-015

Question: Which of the following are the main factors that affect the selection of an alternate location during the development of a DRP? (Choose all that apply.)

A: geographic location
B: organizational needs
C: location's cost
D: location's restoration effort

Answer(s): A,B,C,D

Explanation: The main factors that affect the selection of an alternate location during the development of a disaster recovery plan (DRP) include the following:

- Geographic location
- Organizational needs
- Location's cost
- Location's restoration effort

Question ID: CISSP-2018-CQ-08-001

Question: Which of the following is the last step in the System Development Life Cycle?

A: Operate/Maintain
B: Dispose
C: Acquire/Develop
D: Initiate

Answer(s): B

Explanation: The five steps in the System Development Life Cycle are as follows:

1. Initiate
2. Acquire/Develop
3. Implement
4. Operate/Maintain
5. Dispose

Question ID: CISSP-2018-CQ-08-002

Question: In which of the following stages of the Software Development Life Cycle is the software actually coded?

A: Gather Requirements
B: Design
C: Develop
D: Test/Validate

Answer(s): C

Explanation: The Develop stage involves writing the code or instructions that make the software work. The emphasis of this phase is strict adherence to secure coding practice.

Question ID: CISSP-2018-CQ-08-003

Question: Which of the following initiatives was developed by the Department of Homeland Security?

A: WASC
B: BSI
C: OWASP
D: ISO

Answer(s): B

Explanation: The Department of Homeland Security (DHS) is involved in promoting software security best practices. The Build Security In (BSI) initiative promotes a process-agnostic approach that makes security recommendations with regard to architectures, testing methods, code reviews, and management processes.

Question ID: CISSP-2018-CQ-08-004

Question: Which of the following development models includes no formal control mechanisms to provide feedback?

A: Waterfall
B: V-Shaped
C: Build and Fix
D: Spiral

Answer(s): C

Explanation: Though it's not a formal model, the Build and Fix approach describes a method that has been largely discredited and is now used as a template for how not to manage a

development project. Simply put, using this method, the software is developed as quickly as possible and released.

Question ID: CISSP-2018-CQ-08-005

Question: Which language type delivers instructions directly to the processor?

A: assembly languages
B: high-level languages
C: machine languages
D: natural languages

Answer(s): C

Explanation: Machine languages deliver instructions directly to the processor. This was the only type of programming done in the 1950s and uses basic binary instructions, using no complier or interpreter. (These programs convert higher language types to a form that can be executed by the processor.)

Question ID: CISSP-2018-CQ-08-006

Question: Which term describes how many different tasks a module can carry out?

A: polymorphism
B: cohesion
C: coupling
D: data structures

Answer(s): B

Explanation: Cohesion describes how many different tasks a module can carry out. If a module is limited to a small number or a single function, it is said to have high cohesion. Coupling describes how much interaction one module requires from another module to do its job. Low or loose coupling indicates that a module does not need much help from other modules, whereas high coupling indicates the opposite.

Question ID: CISSP-2018-CQ-08-007

Question: Which term describes a standard for communication between processes on the same computer?

A: CORBA
B: DCOM
C: COM
D: SOA

Answer(s): C

Explanation: Component Object Model (COM) is a model for communication between processes on the same computer, while as the name implies, the Distributed Component Object Model (DCOM) is a model for communication between processes in different parts of the network.

Question ID: CISSP-2018-CQ-08-008

Question: Which of the following is a Microsoft technology?

A: ActiveX
B: Java
C: SOA
D: CORBA

Answer(s): A

Explanation: ActiveX is a Microsoft technology that uses object-oriented programming (OOP) and is based on the COM and DCOM.

Question ID: CISSP-2018-CQ-08-009

Question: Which of the following is the dividing line between the trusted parts of the system and those that are untrusted?

A: security perimeter
B: reference monitor
C: trusted computer base (TCB)
D: security kernel

Answer(s): A

Explanation: The security perimeter is the dividing line between the trusted parts of the system and those that are untrusted. According to security design best practices, components that lie within this boundary (which means they lie within the TCB) should never permit untrusted components to access critical resources in an insecure manner.

Question ID: CISSP-2018-CQ-08-010

Question: Which of the following is a system component that enforces access controls on an object?

A: security perimeter
B: reference monitor
C: trusted computer base (TCB)

D: security kernel

Answer(s): B

Explanation: A reference monitor is a system component that enforces access controls on an object. It is an access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Question ID: CISSP-2018-CQ-08-011

Question: Which of the following ensures that the customer (either internal or external) is satisfied with the functionality of the software?

A: Integration testing
B: Acceptance testing
C: Regression testing
D: Accreditation

Answer(s): B

Explanation: Acceptance testing ensures that the customer (either internal or external) is satisfied with the functionality of the software. Integration testing assesses how the modules work together and determines whether functional and security specifications have been met. Regression testing takes places after changes are made to the code to ensure that the changes have reduced neither functionality nor security. Accreditation is the formal acceptance of the adequacy of a system's overall security by management.

Question ID: CISSP-2018-CQ-08-012

Question: In which of the following models is less time spent on the upfront analysis and more emphasis placed on learning from the process feedback and incorporating lessons learned in real time?

A: Agile
B: Rapid Application Development
C: Cleanroom
D: Modified Waterfall

Answer(s): A

Explanation: With the Agile model, less time is spent on upfront analysis and more emphasis is placed on learning from the process and incorporating lessons learned in real time. There is also more interaction with the customer throughout the process. In the Rapid Application Development (RAD) model, less time is spent upfront on design, while emphasis is placed on rapidly producing prototypes with the assumption that crucial knowledge can only be gained through trial and error. In contrast to the JAD model, the Cleanroom model strictly adheres to

formal steps and a more structured method. It attempts to prevent errors and mistakes through extensive testing. In the modified Waterfall model, each phase in the development process is considered its own milestone in the project management process. Unlimited backward iteration (returning to earlier stages to address problems) is not allowed in this model.

Question ID: CISSP-2018-CQ-08-013

Question: Which of the following software development risk analysis and mitigation strategy guidelines should security professionals follow? (Choose all that apply.)

A: Integrate risk analysis and mitigation in the Software Development Life Cycle.
B: Use qualitative, quantitative, and hybrid risk analysis approaches based on standardized risk analysis methods.
C: Track and manage weaknesses that are discovered throughout risk assessment, change management, and continuous monitoring.
D: Encapsulate data to make it easier to apply the appropriate policies to objects.

Answer(s): A,B,C

Explanation: Security professionals should ensure that the software development risk analysis and mitigation strategy follows these guidelines:

- Integrate risk analysis and mitigation in the Software Development Life Cycle.
- Use qualitative, quantitative, and hybrid risk analysis approaches based on standardized risk analysis methods.
- Track and manage weaknesses that are discovered throughout risk assessment, change management, and continuous monitoring.

Question ID: CISSP-2018-CQ-08-014

Question: Which of the following are valid guidelines for providing API security? (Choose all that apply.)

A: Use the same security controls for APIs as any web application on the enterprise.
B: Use Hash-based Message Authentication Code (HMAC).
C: Use encryption when passing static keys.
D: Implement password encryption instead of single key-based authentication.

Answer(s): A,B,C,D

Explanation: Comprehensive security must protect the entire spectrum of devices in the digital workplace, including apps and APIs. API security is critical for an organization that is exposing digital assets. Guidelines for providing API security include:

- Use the same security controls for APIs as for any web application on the enterprise.
- Use Hash-based Message Authentication Code (HMAC).
- Use encryption when passing static keys.

- Use a framework or an existing library to implement security solutions for APIs.
- Implement password encryption instead of single key-based authentication.

Question ID: CISSP-2018-CQ-08-015

Question: Which of the following is NOT one of the four phases of acquiring software?

A: Planning
B: Contracting
C: Development
D: Monitoring and accepting

Answer(s): C

Explanation: In the Software Development Life Cycle, the code or instructions that make the software work is written in the Develop phase. The process of acquiring software has the following four phases:

1. *Planning:* During this phase, the organization performs a needs assessment, develops the software requirements, creates the acquisition strategy, and develops evaluation criteria and plan.

2. *Contracting:* Once planning is complete, the organization creates a request for proposal (RFP) or other supplier solicitation forms, evaluates the supplier proposals, and negotiates the final contract with the selected seller.

3. *Monitoring and accepting*: When a contract is in place, the organization establishes the contract work schedule, implements change control procedures, and reviews and accepts the software deliverables.

4. *Follow-up:* When the software is in place, the organization must sustain the software, including managing risks and changes. At some point, it may be necessary for the organization to decommission the software.

Question ID: CISSP-2018-RA-01-1-061

Question: Which term is used for an instance of being subjected to losses from a threat?

A: Safeguard
B: Vulnerability
C: Exposure
D: Trigger

Answer(s): C

Explanation: An exposure is an instance of being subjected or exposed to losses from a threat. A safeguard is a control designed to counteract a threat. A vulnerability is a flaw or weakness in the system, software, or hardware. A trigger is an event that indicates that a risk has occurred or is about to occur.

Question ID: CISSP-2018-RA-01-1-062

Question: Which term is used for an event that indicates that a risk has occurred or is about to occur?

A: Safeguard
B: Vulnerability
C: Exposure
D: Trigger

Answer(s): D

Explanation: A trigger is an event that indicates that a risk has occurred or is about to occur. A safeguard is a control designed to counteract a threat. A vulnerability is a flaw or weakness in the system, software, or hardware. An exposure is an instance of being subjected or exposed to losses from a threat.

Question ID: CISSP-2018-RA-01-1-063

Question: What are the detailed instructions used to accomplish a task or a goal?

A: Procedures
B: Standards
C: Guidelines
D: Baselines

Answer(s): A

Explanation: Procedures are the detailed instructions used to accomplish a task or goal. Standards are the mandated rules that govern the acceptable level of security. Guidelines are the actions that are suggested when standards are not applicable in a particular situation. Baselines define the minimum level of security or performance.

Question ID: CISSP-2018-RA-01-1-064

Question: What are the mandated rules that govern the acceptable level of security?

A: Procedures
B: Standards
C: Guidelines
D: Baselines

Answer(s): B

Explanation: Standards are the mandated rules that govern the acceptable level of security. Procedures are the detailed instructions used to accomplish a task or goal. Guidelines are the actions that are suggested when standards are not applicable in a particular situation. Baselines define the minimum level of security or performance.

Question ID: CISSP-2018-RA-01-1-065

Question: Which of the following is a process management development standard?

A: NIST SP 800-53
B: Zachman framework
C: ITIL
D: ISO 27000

Answer(s): C

Explanation: ITIL is a process management development standard. NIST SP 800-53 is a security controls development framework. The Zachman framework is an enterprise architecture framework. ISO 27000 is a security program development standard.

Question ID: CISSP-2018-RA-01-1-066

Question: Which of the following is a security program development standard?

A: NIST SP 800-53
B: Zachman framework
C: ITIL
D: ISO 27000

Answer(s): D

Explanation: ISO 27000 is a security program development standard. NIST SP 800-53 is a security controls development framework. The Zachman framework is an enterprise architecture framework. ITIL is a process management development standard.

Question ID: CISSP-2018-RA-01-1-067

Question: During which stage of the security program life cycle do you obtain management approval?

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

Answer(s): A

Explanation: You obtain management approval during the Plan and Organize stage of the security program life cycle. All the other stages of the security program life cycle occur after you obtain management approval.

Question ID: CISSP-2018-RA-01-1-068

Question: During which stage of the security program life cycle do you identify assets?

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

Answer(s): B

Explanation: You identify assets during the Implement stage of the security program life cycle. None of the other stages are responsible for identifying assets.

Question ID: CISSP-2018-RA-01-1-069

Question: When designing the security awareness training for your organization, which group needs their training to focus on the risk to the organization and the laws and regulations that affect the organization?

A: Technical staff
B: Regular staff
C: Senior management
D: Middle management

Answer(s): C

Explanation: When designing the security awareness training for your organization, senior management needs the training to focus on the risk to the organization and the laws and regulations that affect the organization. Technical staff needs the security awareness training to focus on configuring and maintaining security controls, including how to recognize an attack when it occurs. Regular staff needs the security awareness training to focus on its responsibilities regarding security so that it performs its day-to-day tasks in a secure manner. Middle management needs the security awareness training to focus on the policies, standards, baselines, guidelines, and procedures that affect security.

Question ID: CISSP-2018-RA-01-1-070

Question: When designing the security awareness training for your organization, which group needs its training to focus on the policies, standards, baselines, guidelines, and procedures that affect security?

A: Technical staff
B: Regular staff
C: Senior management
D: Middle management

Answer(s): D

Explanation: When designing the security awareness training for your organization, middle management needs the training to focus on the policies, standards, baselines, guidelines, and procedures that affect security. Technical staff needs the security awareness training to focus on configuring and maintaining security controls, including how to recognize an attack when it occurs. Regular staff needs the security awareness training to focus on its responsibilities regarding security so that it performs its day-to-day tasks in a secure manner. Senior management needs the security awareness training to focus on the risk to the organization and the laws and regulations that affect the organization.

Question ID: CISSP-2018-RA-01-1-081

Question: Which business continuity document considers all aspects that are affected by a disaster, including functions, systems, personnel, and facilities, and lists and prioritizes the services that are needed?

A: BIA
B: Contingency plan
C: BCP
D: DRP

Answer(s): C

Explanation: The business continuity plan (BCP) considers all aspects that are affected by a disaster, including functions, systems, personnel, and facilities, and lists and prioritizes the services that are needed. A business impact analysis (BIA) is a functional analysis that lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization. A contingency plan provides instruction on what personnel should do until the functions and systems are restored to full functionality. A disaster recovery plan (DRP) is implemented when the emergency occurs and includes the steps to restore functions and systems.

Question ID: CISSP-2018-RA-01-1-082

Question: Which business continuity document is implemented when the emergency occurs and includes the steps to restore functions and systems?

A: BIA
B: Contingency plan
C: BCP
D: DRP

Answer(s): D

Explanation: A disaster recovery plan (DRP) is implemented when the emergency occurs and includes the steps to restore functions and systems. A business impact analysis (BIA) is a functional analysis that lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization. A contingency plan provides instruction on what personnel should do until the functions and systems are restored to full functionality. The business continuity plan (BCP) considers all aspects that are affected by a disaster, including functions, systems, personnel, and facilities, and lists and prioritizes the services that are needed.

Question ID: CISSP-2018-RA-01-1-083

Question: As part of the process of conducting a business impact analysis (BIA), you are creating a list of all the business assets. Which step of the BIA are you performing?

A: Identify critical processes and resources.
B: Identify resource requirements.
C: Identify outage impacts, and estimate downtime.
D: Identify recovery priorities.

Answer(s): A

Explanation: You are performing the step to identify critical processes and resources of the BIA. During the identify resource requirements step, you would document the device name, operating system or platform version, hardware requirements, and device interrelationships of all devices. During the identify outage impacts and estimate downtime step, you would perform the MTD, MTTR, and MTBF calculations. During the identify recovery priorities step, you would take into account all the recovery calculations to produce a recovery hierarchy.

Question ID: CISSP-2018-RA-01-1-084

Question: As part of the process of conducting a business impact analysis (BIA), you document the device name, operating system or platform version, hardware requirements, and device interrelationships of all devices. Which step of the BIA are you performing?

A: Identify critical processes and resources.
B: Identify resource requirements.
C: Identify outage impacts, and estimate downtime
D: Identify recovery priorities.

Answer(s): B

Explanation: During the identify resource requirements step, you would document the device name, operating system or platform version, hardware requirements, and device interrelationships of all devices. During the identify critical processes and resources step, you create a list of all the business assets. During the identify outage impacts and estimate downtime step, you would perform the MTD, MTTR, and MTBF calculations. During the identify recovery priorities step, you would take into account all the recovery calculations to produce a recovery hierarchy.

Question ID: CISSP-2018-RA-01-1-092

Question: You are responsible for investigating all computer crime that occurs against your organization. What is the biggest hindrance to your investigations?

A: Computer criminals employ more sophisticated tools than computer investigators.
B: Computer crime has no borders or jurisdictions.
C: Fighting computer crime is often underfunded.
D: Most computer crime cannot be prosecuted.

Answer(s): B

Explanation: The biggest hindrance to computer investigations is that computer crime has no borders or jurisdictions. Criminals can literally be anywhere. Most of the same tools that are available to computer criminals are also available to computer investigators. Although fighting

computer crime can be underfunded, this is not the biggest hindrance. Most computer crime can be prosecuted provided that the evidence has been collected and preserved in a proper manner.

Question ID: CISSP-2018-RA-01-1-101

Question: Which of the following statements regarding the CIA triad are TRUE?

A: Confidentiality ensures that data is not disclosed to unauthorized entities.
B: The opposite of integrity is corruption.
C: Availability ensures that data is accessible when it is needed.
D: Statements a and b only
E: Statements b and c only
F: All the statements
G: None of the statements

Answer(s): F

Explanation: All the statements are correct. Confidentiality ensures that data is not disclosed to unauthorized entities. The opposite of integrity is corruption. Availability ensures that data is accessible when it is needed.

Question ID: CISSP-2018-RA-01-1-102

Question: What are the three main concepts for the security of information assets?

A: Confidentiality, integrity, and availability
B: Confidentiality, integrity, and authentication
C: Confidentiality, integrity, and accountability
D: Risks, threats, and vulnerabilities

Answer(s): A

Explanation: The three main concepts for the security of information assets are confidentiality, integrity, and availability.

Question ID: CISSP-2018-RA-01-1-103

Question: Your organization has recently decided to develop a comprehensive security program. The security program has been authorized by management. What is the first step in this process?

A: Define the scope of the security program.
B: Identify the assets that require protection.
C: Determine the level of protection each asset needs.

D: Determine the responsibilities of personnel.
E: Develop consequences for noncompliance.

Answer(s): A

Explanation: After management approval has been given, the steps in developing a comprehensive security program are as follows: 1. Define the scope of the security program. 2. Identify all the assets that need protection. 3. Determine the level of protection that each asset needs. 4. Determine personnel responsibilities. 5. Develop consequences for noncompliance with the security policy.

Question ID: CISSP-2018-RA-01-1-104

Question: Your organization has put all policies, procedures, and standards into place as a result of a security audit. Which security tenet did the organization fulfill by doing this?

A: Due care
B: Due diligence
C: Confidentiality
D: Integrity

Answer(s): A

Explanation: Your organization fulfilled the due care tenet by putting into place all the recommended policies, procedures, and standards. None of the other tenets are described in this scenario.

Question ID: CISSP-2018-RA-01-1-105

Question: When an organization fails to do all it can to protect its employees' PII, it has exhibited which concept?

A: Due care
B: Due diligence
C: REP
D: Negligence

Answer(s): D

Explanation: The listed terns are defined as follows: Due diligence: Means that an organization understands the security risks that it faces. Due diligence then provides the information necessary to ensure that the organization practices due care. Due care: Is all about action. Organizations must institute the appropriate protections and procedures for all organizational assets, especially

intellectual property. If an organization does not take actions that a prudent person would have taken under similar circumstances, the organization is negligent. REP (reasonable expectation of privacy): Many organizations implement a No Expectation of Privacy policy that the employee must sign after receiving the appropriate training. Keep in mind that this policy should specifically describe any unacceptable behavior. Negligence: A failure to exercise due care or to institute the appropriate protections and procedures for all organizational assets, including employees.

Question ID: CISSP-2018-RA-01-1-107

Question: You are the security analyst for a healthcare provider. You need to ensure that your company complies with all governmental laws and regulations. Which of the following must you consider as part of your security plan?

A: HIPAA
B: DoDAF
C: MODAF
D: SOX

Answer(s): A

Explanation: You must consider the Health Insurance Portability and Accountability Act (HIPAA) because you work for a healthcare provider.

Question ID: CISSP-2018-RA-01-1-108

Question: Which document is an agreement between a software vendor and a business customer, such as a company or organization, specifying terms of use

A: Software license agreement
B: End user license agreement
C: Nondisclosure agreement
D: Acceptable use policy

Answer(s): A

Explanation: The listed agreements cover the following issues: Acceptable use policy: An agreement that includes information regarding no expectation of privacy, meaning that usage of the computer is not private and usually includes a restriction that forbids users in an organization from installing unauthorized software. Software license agreement: An agreement between a software vendor and a business customer specifying terms of use. End user license agreement: An agreement between a software vendor and the end user, usually the computer owner. Nondisclosure agreement: An agreement between two parties that information being shared will

not be disclosed to third parties.

Question ID: CISSP-2018-RA-01-1-109

Question: Which document is an agreement between a software vendor and the home computer owner?

A: Software license agreement
B: End user license agreement
C: Nondisclosure agreement
D: Acceptable use policy

Answer(s): B

Explanation: The listed agreements cover the following issues: Acceptable use policy: An agreement that includes information regarding no expectation of privacy, meaning that usage of the computer is not private and usually includes a restriction that forbids users in an organization from installing unauthorized software. Software license agreement: An agreement between a software vendor and a business customer specifying terms of use. End user license agreement: An agreement between a software vendor and the end user, usually the computer owner. Nondisclosure agreement: An agreement between two parties that information being shared will not be disclosed to third parties.

Question ID: CISSP-2018-RA-01-1-110

Question: Which statement BEST describes the Internet Architecture Board (IAB)?

A: It maintains an ethics-related statement concerning the use of the Internet.
B: It is a group dedicated to making the Internet better.
C: It develops standards for new technologies, including wireless.
D: It is responsible for the allocation of IP addresses and management of DNS.

Answer(s): A

Explanation: The IAB maintains an ethics-related statement concerning the use of the Internet. The Internet Engineering Task Force (IETF) is a group dedicated to making the Internet better. The Institute of Electrical and Electronics Engineers (IEEE) develops standards for new technologies, including wireless. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the allocation of IP addresses and management of DNS.

Question ID: CISSP-2018-RA-01-1-111

Question: Which statement BEST describes the Internet Engineering Task Force (IETF)?

A: It maintains an ethics-related statement concerning the use of the Internet.
B: It is a group dedicated to making the Internet better.
C: It develops standards for new technologies, including wireless.
D: It is responsible for the allocation of IP addresses and management of DNS.

Answer(s): B

Explanation: The Internet Engineering Task Force (IETF) is a group dedicated to making the Internet better. The Internet Architecture Board (IAB) maintains an ethics-related statement concerning the use of the Internet. The Institute of Electrical and Electronics Engineers (IEEE) develops standards for new technologies, including wireless. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the allocation of IP addresses and management of DNS.

Question ID: CISSP-2018-RA-01-1-112

Question: Which of the following statements regarding security policies are TRUE?

A: An organizational security must be supported by all stakeholders.
B: An organizational security policy must be established by management.
C: An organizational security policy should be reviewed on a regular basis.
D: An organizational security policy should control the business objectives.
E: Statements a, b, and c only
F: Statements b, c, and d only
G: All the statements

Answer(s): E

Explanation: The following statements are TRUE regarding security policies: An organizational security must be supported by all stakeholders. An organizational security policy must be established by management. An organizational security policy should be reviewed on a regular basis. An organizational security policy should NOT control the business objectives. The business objectives should control the organizational security policy.

Question ID: CISSP-2018-RA-01-1-113

Question: Which of the following is NOT an issue-specific policy?

A: E-mail retention policy
B: Auditing policy
C: File server logout policy
D: Acceptable use policy

E: Statements a, b, and c only
F: Statements a, c, and d only
G: All the statements

Answer(s): C

Explanation: A file server logout policy is NOT an issue-specific policy. It is considered a system-specific policy because it covers a specific set of systems. All the other listed policies are issue-specific policies because they address a particular issue or function.

Question ID: CISSP-2018-RA-01-1-114

Question: You have been asked to develop the business continuity plan and scope. You are working with a team with members from each organizational department. The team has a list of different scenarios that may require the development of a disaster recovery plan. Which of the following scenarios is NOT important as part of this plan?

A: Hardware failure
B: Employee termination
C: Natural disaster
D: Hardware relocation
E: Statements a and c
F: Statements b and d
G: All the statements

Answer(s): F

Explanation: As a part of the business continuity plan, you do not have to include employee termination or hardware relocation as part of the disaster recovery plan. These events are considered events that occur during normal operation. Hardware failure and natural disasters will require the development of a disaster recovery plan.

Question ID: CISSP-2018-RA-01-1-115

Question: You are assembling the business continuity project scope and plan. Which of the following guidelines should you NOT consider?

A: The business continuity team should include members from all organizational departments.
B: The business continuity plan should consider all aspects of the organization.
C: Senior management should endorse any business continuity plan that is adopted.
D: The scope of the project should be properly defined first.
E: None of the statements
F: All the statements

Answer(s): E

Explanation: None of the statements should NOT be considered as part of the business continuity project scope and plan. All the statements should be used as guidelines for the business continuity project scope and plan.

Question ID: CISSP-2018-RA-01-1-116

Question: What is the first step of business continuity?

A: Develop the contingency plan.
B: Develop recovery strategies.
C: Identify preventative controls.
D: Develop the continuity planning policy statement.

Answer(s): D

Explanation: The first step of business continuity is to develop the continuity planning policy statement. All the other listed statements should be completed only after the continuity planning policy statement has been written.

Question ID: CISSP-2018-RA-01-1-117

Question: Which of the following should NOT be completed prior to hiring new personnel?

A: Education verification
B: Work history verification
C: Professional licensing verification
D: Employee training verification
E: None of the options

Answer(s): D

Explanation: Employee training verification should NOT be completed prior to hiring new personnel. Employee training is performed AFTER personnel is hired.

Question ID: CISSP-2018-RA-01-1-118

Question: Which of the following should NOT be included in the procedures for unfriendly personnel termination?

A: Security escort from the premises

B: System and facility access removal following the termination
C: Immediate seizure of all company assets
D: Statements a and b only
E: Statements b and c only
F: Statements a and c only
G: None of the statements

Answer(s): B

Explanation: System and facility access removal following the termination should NOT be included. System and facility access removal should occur immediately BEFORE the termination.

Question ID: CISSP-2018-RA-01-1-119

Question: Which of the following statements are TRUE regarding access control categories?

A: Corrective controls include data backups and fire extinguishers.
B: Detective controls include guards and audit logs.
C: Deterrent controls include NDAs and fencing.
D: Preventive controls include antivirus software and guards.
E: Statements a, b, and c only
F: Statements a, c, and d only
G: All the statements

Answer(s): G

Explanation: All the given statements are correct. Corrective controls include data backups and fire extinguishers. Detective controls include guards and audit logs. Deterrent controls include NDAs and fencing, and preventive controls include antivirus software and guards. Guards act as both detective controls and preventive controls.

Question ID: CISSP-2018-RA-01-1-120

Question: Which of the following statements regarding administrative controls are FALSE?

A: Detective administrative controls include job rotation and background checks.
B: Preventive administrative controls include personnel procedures and security awareness training.
C: Recovery administrative controls include disaster recovery plans and data backups.
D: Statements a and b only
E: Statements b and c only
F: All the statements

G: None of the statements

Answer(s): C

Explanation: Recovery administrative controls do NOT include data backups. Data backups are recovery logical controls. Disaster recovery plans are recovery administrative controls. Detective administrative controls include job rotation and background checks. Preventive administrative controls include personnel procedures and security awareness training.

Question ID: CISSP-2018-RA-01-1-121

Question: Which statements regarding threat modeling are TRUE?

A: Threat modeling begins with understanding the systems that are implemented by the organization.
B: Identifying assets and access points is a critical step in the threat modeling process.
C: The final step is to identify the threats.
D: Statements a and b only
E: Statements b and c only
F: Statements a and c only
G: All the statements

Answer(s): G

Explanation: All the statements regarding threat modeling are true.

Question ID: CISSP-2018-RA-01-1-122

Question: During threat modeling, organizations must identify access points that can be threatened. Which of the following access points should be identified?

A: Open sockets
B: Hardware ports
C: Trust boundaries
D: Statements a and b only
E: Statements b and c only
F: Statements a and c only
G: All the statements

Answer(s): G

Explanation: All the statements given are access points that should be identified during threat modeling.

Question ID: CISSP-2018-RA-01-1-123

Question: Threats are often classified into six categories: spoofing, tampering, repudiation, information disclosure, denial- of-service, and elevation of privilege. Which of these categories involves the changing of data to carry out an attack?

A: Spoofing
B: Tampering
C: Repudiation
D: Information disclosure
E: Denial-of-service
F: Escalation of privilege

Answer(s): B

Explanation: Tampering involves the changing of data to carry out an attack. Spoofing involves using someone else's credentials to gain access to assets. Repudiation occurs when a user denies performing an action, and there is no way to prove that the user carried out an action. Information disclosure occurs when information is given to unauthorized users. Denial-of-service occurs when valid users are denied access to an asset they legitimately need. Escalation of privilege occurs when a user obtains a higher level of access to an asset than he should have.

Question ID: CISSP-2018-RA-01-1-124

Question: Threats are often classified into six categories: spoofing, tampering, repudiation, information disclosure, denial-of-service, and elevation of privilege. Which of these categories involves being unable to prove that a user carried out a certain action?

A: Spoofing
B: Tampering
C: Repudiation
D: Information disclosure
E: Denial-of-service
F: Escalation of privilege

Answer(s): C

Explanation: Repudiation occurs when a user denies performing an action, and there is no way to prove that the user carried out an action. Spoofing involves using someone else's credentials to gain access to assets. Tampering involves the changing of data to carry out an attack. Information disclosure occurs when information is given to unauthorized users. Denial-of-service occurs when valid users are denied access to an asset they legitimately need. Escalation

of privilege occurs when a user obtains a higher level of access to an asset than he should have.

Question ID: CISSP-2018-RA-01-1-125

Question: Threats are often classified into six categories: spoofing, tampering, repudiation, information disclosure, denial-of-service, and elevation of privilege. Which of these categories involves using another person's credentials to access an organization's assets?

A: Spoofing
B: Tampering
C: Repudiation
D: Information disclosure
E: Denial-of-service
F: Escalation of privilege

Answer(s): A

Explanation: Spoofing involves using someone else's credentials to gain access to assets. Tampering involves the changing of data to carry out an attack. Repudiation occurs when a user denies performing an action, and there is no way to prove that the user carried out an action. Information disclosure occurs when information is given to unauthorized users. Denial-of-service occurs when valid users are denied access to an asset they legitimately need. Escalation of privilege occurs when a user obtains a higher level of access to an asset than he should have.

Question ID: CISSP-2018-RA-01-1-126

Question: Threats are often classified into six categories: spoofing, tampering, repudiation, information disclosure, denial-of-service, and elevation of privilege. Which of these categories involves a valid user being denied access to an asset that they can normally access?

A: Spoofing
B: Tampering
C: Repudiation
D: Information disclosure
E: Denial-of-service
F: Escalation of privilege

Answer(s): E

Explanation: Denial-of-service occurs when valid users are denied access to an asset they legitimately need. Spoofing involves using someone else's credentials to gain access to assets. Tampering involves the changing of data to carry out an attack. Repudiation occurs when a user denies performing an action, and there is no way to prove that the user carried out an action.

Information disclosure occurs when information is given to unauthorized users. Escalation of privilege occurs when a user obtains a higher level of access to an asset than he should have.

Question ID: CISSP-2018-RA-01-1-127

Question: Threats are often classified into six categories: spoofing, tampering, repudiation, information disclosure, denial-of-service, and elevation of privilege. Which of these categories occurs when a user has obtained read-and-write permissions to an asset that the user should only be able to read?

A: Spoofing
B: Tampering
C: Repudiation
D: Information disclosure
E: Denial-of-service
F: Escalation of privilege

Answer(s): F

Explanation: Escalation of privilege occurs when a user obtains a higher level of access to an asset than he should have. Spoofing involves using someone else's credentials to gain access to assets. Tampering involves the changing of data to carry out an attack. Repudiation occurs when a user denies performing an action, and there is no way to prove that the user carried out an action. Information disclosure occurs when information is given to unauthorized users. Denial-of-service occurs when valid users are denied access to an asset they legitimately need.

Question ID: CISSP-2018-RA-01-1-128

Question: Why is it important to audit a third party's access to internal resources?

A: To determine the level of access needed by the third party
B: To determine third-party compliance with organizational security policies and standards
C: To determine if appropriate and inappropriate actions are being carried out by third-party personnel
D: To document the guidelines that the third party will follow

Answer(s): C

Explanation: It is important to audit a third party's access to internal resources to determine if appropriate and inappropriate actions are being carried out by third-party personnel.

Question ID: CISSP-2018-RA-01-1-129

Question: At which time should new personnel be given security awareness training?

A: At termination
B: At hiring
C: At the next regularly scheduled session
D: After completing the probation period

Answer(s): B

Explanation: New personnel should be given security awareness training at hiring.

Question ID: CISSP-2018-RA-01-1-130

Question: What is the main focus of security awareness training?

A: How security is implemented
B: Why security is important
C: Who implements security
D: When security is important

Answer(s): B

Explanation: The main focus of security awareness training is why security is important.

Question ID: CISSP-2018-RA-01-2-003

Question: A governmental agency decides that it must digitally sign certain e-mail messages that are sent. Which tenet will this cover?

A: Confidentiality
B: Integrity
C: Availability
D: Accountability

Answer(s): B

Explanation: Digitally signing e-mail messages will cover the integrity tenet. It also provides authentication and non-repudiation.

Question ID: CISSP-2018-RA-01-2-061

Question: Which term is used for a control designed to counteract a threat?

A: Safeguard
B: Vulnerability
C: Exposure
D: Trigger

Answer(s): A

Explanation: A safeguard is a control designed to counteract a threat. A vulnerability is a flaw or weakness in the system, software, or hardware. An exposure is an instance of being subjected or exposed to losses from a threat. A trigger is an event that indicates that a risk has occurred or is about to occur.

Question ID: CISSP-2018-RA-01-2-062

Question: Which term is used for a flaw or weakness in the system, software, or hardware?

A: Safeguard
B: Vulnerability
C: Exposure
D: Trigger

Answer(s): B

Explanation: A vulnerability is a flaw or weakness in the system, software, or hardware. A safeguard is a control designed to counteract a threat. An exposure is an instance of being subjected or exposed to losses from a threat. A trigger is an event that indicates that a risk has occurred or is about to occur.

Question ID: CISSP-2018-RA-01-2-063

Question: What are the actions that are suggested when standards are not applicable in a particular situation?

A: Procedures
B: Standards
C: Guidelines
D: Baselines

Answer(s): C

Explanation: Guidelines are the actions that are suggested when standards are not applicable in a particular situation. Procedures are the detailed instructions used to accomplish a task or goal. Standards are the mandated rules that govern the acceptable level of security. Baselines define

the minimum level of security or performance.

Question ID: CISSP-2018-RA-01-2-064

Question: What defines the minimum level of security or performance?

A: Procedures
B: Standards
C: Guidelines
D: Baselines

Answer(s): D

Explanation: Baselines define the minimum level of security or performance. Procedures are the detailed instructions used to accomplish a task or goal. Standards are the mandated rules that govern the acceptable level of security. Guidelines are the actions that are suggested when standards are not applicable in a particular situation.

Question ID: CISSP-2018-RA-01-2-065

Question: Which of the following is a security controls development framework?

A: NIST SP 800-53
B: Zachman framework
C: ITIL
D: ISO 27000

Answer(s): A

Explanation: NIST SP 800-53 is a security controls development framework. The Zachman framework is an enterprise architecture framework. ITIL is a process management development standard. ISO 27000 is a security program development standard.

Question ID: CISSP-2018-RA-01-2-066

Question: Which of the following is an enterprise architecture framework?

A: NIST SP 800-53
B: Zachman framework
C: ITIL
D: ISO 27000

Answer(s): B

Explanation: The Zachman framework is an enterprise architecture framework. NIST SP 800-53 is a security controls development framework. ITIL is a process management development standard. ISO 27000 is a security program development standard.

Question ID: CISSP-2018-RA-01-2-067

Question: During which stage of the security program life cycle do you perform audits?

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

Answer(s): C

Explanation: You perform audits during the Operate and Maintain stage of the security program life cycle. None of the other stages are responsible for performing audits.

Question ID: CISSP-2018-RA-01-2-068

Question: During which stage of the security program life cycle do you review audit logs?

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

Answer(s): D

Explanation: You review audit logs during the Monitor and Evaluate stage of the security program life cycle. None of the other stages are responsible for reviewing audit logs.

Question ID: CISSP-2018-RA-01-2-069

Question: When designing the security awareness training for your organization, which group needs its training to focus on configuring and maintaining security controls, including how to recognize an attack when it occurs?

A: Technical staff
B: Regular staff
C: Senior management
D: Middle management

Answer(s): A

Explanation: When designing the security awareness training for your organization, technical staff needs the training to focus on configuring and maintaining security controls, including how to recognize an attack when it occurs. Regular staff needs the security awareness training to focus on its responsibilities regarding security so that it performs its day-to-day tasks in a secure manner. Senior management needs the security awareness training to focus on the risk to the organization and the laws and regulations that affect the organization. Middle management needs the security awareness training to focus on the policies, standards, baselines, guidelines, and procedures that affect security.

Question ID: CISSP-2018-RA-01-2-070

Question: When designing the security awareness training for your organization, which group needs its training to focus on its responsibilities regarding security so that it performs its day-to-day tasks in a secure manner?

A: Technical staff
B: Regular staff
C: Senior management
D: Middle management

Answer(s): A

Explanation: When designing the security awareness training for your organization, regular staff needs the training to focus on configuring and maintaining security controls, including how to recognize an attack when it occurs. Technical staff needs the security awareness training to focus on its responsibilities regarding security so that it performs its day-to-day tasks in a secure manner. Senior management needs the security awareness training to focus on the risk to the organization and the laws and regulations that affect the organization. Middle management needs the security awareness training to focus on the policies, standards, baselines, guidelines, and procedures that affect security.

Question ID: CISSP-2018-RA-01-2-081

Question: Which business continuity document is a functional analysis that lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization?

A: BIA
B: Contingency plan
C: BCP

D: DRP

Answer(s): A

Explanation: A business impact analysis (BIA) is a functional analysis that lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization. A contingency plan provides instruction on what personnel should do until the functions and systems are restored to full functionality. The business continuity plan (BCP) considers all aspects that are affected by a disaster, including functions, systems, personnel, and facilities, and lists and prioritizes the services that are needed. A disaster recovery plan (DRP) is implemented when the emergency occurs and includes the steps to restore functions and systems.

Question ID: CISSP-2018-RA-01-2-082

Question: Which business continuity document provides instruction on what personnel should do until the functions and systems are restored to full functionality?

A: BIA
B: Contingency plan
C: BCP
D: DRP

Answer(s): B

Explanation: A contingency plan provides instruction on what personnel should do until the functions and systems are restored to full functionality. A business impact analysis (BIA) is a functional analysis that lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization. The business continuity plan (BCP) considers all aspects that are affected by a disaster, including functions, systems, personnel, and facilities, and lists and prioritizes the services that are needed. A disaster recovery plan (DRP) is implemented when the emergency occurs and includes the steps to restore functions and systems.

Question ID: CISSP-2018-RA-01-2-083

Question: As part of the process of conducting a business impact analysis (BIA), you perform the MTD, MTTR, and MTBF calculations. Which step of the BIA are you performing?

A: Identify critical processes and resources.
B: Identify resource requirements.
C: Identify outage impacts, and estimate downtime.
D: Identify recovery priorities.

Answer(s): C

Explanation: During the identify outage impacts and estimate downtime step, you would perform the MTD, MTTR, and MTBF calculations. During the identify critical processes and resources step, you create a list of all the business assets. During the identify resource requirements step, you would document the device name, operating system or platform version, hardware requirements, and device interrelationships of all devices. During the identify recovery priorities step, you would take into account all the recovery calculations to produce a recovery hierarchy.

Question ID: CISSP-2018-RA-01-2-084

Question: As part of the process of conducting a business impact analysis (BIA), you take into account all the recovery calculations to produce a recovery hierarchy. Which step of the BIA are you performing?

A: Identify critical processes and resources.
B: Identify resource requirements.
C: Identify outage impacts, and estimate downtime.
D: Identify recovery priorities.

Answer(s): D

Explanation: During the identify recovery priorities step, you would take into account all of the recovery calculations to produce a recovery hierarchy. During the identify critical processes and resources step, you create a list of all the business assets. During the identify resource requirements step, you would document the device name, operating system or platform version, hardware requirements, and device interrelationships of all devices. During the identify outage impacts and estimate downtime step, you would perform the MTD, MTTR, and MTBF calculations.

Question ID: CISSP-2018-RA-01-2-091

Question: What is the Patriot Act?

A: A United States law established in 2001 to reduce restrictions on the searches of telephone, e-mail communications, medical, financial, and other records
B: A type of attack that involved attempting to exploit or corrupt an enemy's information to gain military or economic advantage
C: A United States government program that reduces electronic equipment emanations
D: The U.S. government entity responsible for dealing with federal computer security incidents that occur in civilian agencies

Answer(s): A

Explanation: The Patriot Act is a United States law established in 2001 to reduce restrictions on the searches of telephone, e-mail communications, medical, financial, and other records. Information warfare is a type of attack that involved attempting to exploit or corrupt an enemy's information to gain military or economic advantage. TEMPEST is a United States government program that reduces electronic equipment emanations. The Federal Computer Incident Response Center (FedCIRC) is the U.S. government entity responsible for dealing with federal computer security incidents that occur in civilian agencies.

Question ID: CISSP-2018-RA-01-2-092

Question: What is information warfare?

A: A United States law established in 2001 to reduce restrictions on the searches of telephone, e-mail communications, medical, financial, and other records
B: A type of attack that involved attempting to exploit or corrupt an enemy's information to gain military or economic advantage
C: A United States government program that reduces electronic equipment emanations
D: The U.S. government entity responsible for dealing with federal computer security incidents that occur in civilian agencies

Answer(s): B

Explanation: Information warfare is a type of attack that involved attempting to exploit or corrupt an enemy's information to gain military or economic advantage. The Patriot Act is a United States law established in 2001 to reduce restrictions on the searches of telephone, e-mail communications, medical, financial, and other records. TEMPEST is a United States government program that reduces electronic equipment emanations. The Federal Computer Incident Response Center (FedCIRC) is the U.S. government entity responsible for dealing with federal computer security incidents that occur in civilian agencies.

Question ID: CISSP-2018-RA-01-2-101

Question: The company you work for has decided to implement a server farm for the company’s databases. Which security tenet will this cover?

A: Confidentiality
B: Integrity
C: Availability
D: Accountability

Answer(s): C

Explanation: Implementing a server farm for the company's databases will cover the availability tenet. A server farm is a set of servers that all provide the same functionality. If one of the servers in the farm goes down, the other servers can continue to operate, thereby providing availability of the databases.

Question ID: CISSP-2018-RA-01-2-102

Question: Your company decides to implement hashing to ensure that several crucial files are not changed. Which security tenet will this cover?

A: Confidentiality
B: Integrity
C: Availability
D: Accountability

Answer(s): B

Explanation: Implementing hashing to ensure that several crucial files are not changed will cover the integrity tenet. Hashing will allow you to determine if the file has been changed by comparing the original hash value to a new hash value. If the values match, the file is unchanged. If the values do not match, the file has been changed.

Question ID: CISSP-2018-RA-01-2-103

Question: Your organization performs the appropriate audits and assessments to ensure that the organization is protected. Which security tenet did the organization fulfill be doing this?

A: Due care
B: Due diligence
C: Confidentiality
D: Integrity

Answer(s): B

Explanation: Your organization fulfilled the due diligence tenet by performing the appropriate audits and assessments to ensure that the organization is protected. None of the other tenets are described in this scenario.

Question ID: CISSP-2018-RA-01-2-104

Question: Which approach is recommended for an information security program?

A: Centralized
B: Decentralized
C: Top-down
D: Bottom-up

Answer(s): C

Explanation: A top-down approach is recommended for an information security program.

Question ID: CISSP-2018-RA-01-2-105

Question: Which of the following is information that can be used to identify an employee?

A: REP
B: PCI DSS
C: PII
D: AUP

Answer(s): C

Explanation: The listed acronyms are defined as follows: REP (reasonable expectation of privacy): Many organizations implement a No Expectation of Privacy policy that the employee must sign after receiving the appropriate training. Keep in mind that this policy should specifically describe any unacceptable behavior. Payment Card Industry Data Security Standard (PCI DSS): Affects any organizations that handle cardholder information for the major credit card companies. PII- (personally identifiable information): Information that can be used to identify an individual or employee. AUP (acceptable use policy): Defines unacceptable employee activities.

Question ID: CISSP-2018-RA-01-2-106

Question: Which legislation requires that all assets of the organization, whether substantial or not, be protected?

A: Computer Security Act of 1987
B: Economic Espionage Act of 1996
C: Privacy Act of 1974
D: European Union Principles on Privacy

Answer(s): B

Explanation: The listed pieces of legislation follow: Privacy Act of 1974: Ensures that only authorized persons should have access to personal information and that personal records should

be up to date and accurate. Computer Security Act of 1987: Requires the creation of computer security plans and the appropriate training of system users or owners where the systems house sensitive information. Economic Espionage Act of 1996: Provides a framework to deal with espionage attacks on corporations. According to the Act, all the assets of the organization, whether substantial or not, require protection. European Union Principles on Privacy: States that the data gathered for private individuals should be used only for the purpose for which it is collected.

Question ID: CISSP-2018-RA-01-2-107

Question: Which type of law applies to offenders who violate government laws meant to protect the public?

A: Criminal law
B: Copyright law
C: Administrative law
D: Civil law

Answer(s): A

Explanation: The listed types of law are defined as follows: Civil law: Governs the payment of compensation and fines without sentencing the offenders to jail. Criminal law: Applies to offenders who violate government laws meant to protect the public. The common punishment in a criminal case is a jail sentence for the individual. Copyright law: Grants the right to control either the distribution or the reproduction of his work to an author. Administrative law: Ensures that the companies and individuals adhere to the regulatory standards prescribed by the government.

Question ID: CISSP-2018-RA-01-2-108

Question: Which type of law governs the payment of compensation and fines without sentencing the offenders to jail?

A: Criminal law
B: Copyright law
C: Administrative law
D: Civil law

Answer(s): D

Explanation: The listed types of law are defined as follows: Civil law: Governs the payment of compensation and fines without sentencing the offenders to jail. Criminal law: Applies to offenders who violate government laws meant to protect the public. The common punishment in

a criminal case is a jail sentence for the individual. Copyright law: Grants the right to control either the distribution or the reproduction of his work to an author. Administrative law: Ensures that the companies and individuals adhere to the regulatory standards prescribed by the government.

Question ID: CISSP-2018-RA-01-2-109

Question: What term describes the extent of liability that exists for not exercising due care and diligence?

A: Legal liability
B: Residual risk
C: Downstream liability
D: Total risk

Answer(s): A

Explanation: The listed terms are defined as follows: Legal liability: Extent of liability that exists for not exercising due care and diligence. Residual risk: Risk that remains after implementing countermeasures. Total risk: Risk that exists before implementing countermeasures. Downstream liability: Ensures that organizations working together under a contract are responsible for their information security management and the security controls deployed by each organization.

Question ID: CISSP-2018-RA-01-2-110

Question: Which statement BEST describes the Institute of Electrical and Electronics Engineers (IEEE)?

A: It maintains an ethics-related statement concerning the use of the Internet.
B: It is a group dedicated to making the Internet better.
C: It develops standards for new technologies, including wireless.
D: It is responsible for the allocation of IP addresses and management of DNS.

Answer(s): C

Explanation: The Institute of Electrical and Electronics Engineers (IEEE) develops standards for new technologies, including wireless. The Internet Architecture Board (IAB) maintains an ethics-related statement concerning the use of the Internet. The Internet Engineering Task Force (IETF) is a group dedicated to making the Internet better. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the allocation of IP addresses and management of DNS.

Question ID: CISSP-2018-RA-01-2-111

Question: Which statement BEST describes the Internet Corporation for Assigned Names and Numbers (ICANN)?

A: It maintains an ethics-related statement concerning the use of the Internet.
B: It is a group dedicated to making the Internet better.
C: It develops standards for new technologies, including wireless.
D: It is responsible for the allocation of IP addresses and management of DNS.

Answer(s): D

Explanation: The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the allocation of IP addresses and management of DNS. The Internet Architecture Board (IAB) maintains an ethics-related statement concerning the use of the Internet. The Internet Engineering Task Force (IETF) is a group dedicated to making the Internet better. The Institute of Electrical and Electronics Engineers (IEEE) develops standards for new technologies, including wireless.

Question ID: CISSP-2018-RA-01-2-112

Question: Which of the following is a system-specific policy?

A: Database server security policy
B: Acceptable use policy
C: Auditing policy
D: Personnel hiring/termination policy

Answer(s): A

Explanation: A database server security policy is a system-specific policy because it covers a specific set of systems. All the other listed policies are issue-specific policies.

Question ID: CISSP-2018-RA-01-2-113

Question: Which of the following is mandatory?

A: Regulatory policy
B: Advisory policy
C: Informative policy
D: Guidelines

Answer(s): A

Explanation: A regulatory policy is mandatory. These policies are often dictated by the government or industry.

Question ID: CISSP-2018-RA-01-2-114

Question: Which of the following activities do NOT occur during the initiation stage of the business continuity program?

A: Obtain senior management support.
B: Define the project scope.
C: Define the project objectives.
D: Conduct the business impact analysis.

Answer(s): D

Explanation: Conducting the business impact analysis (BIA) does NOT occur during the initiation stage of the business continuity program. It is the step that you complete after the initiation stage is complete. The initiation stage includes obtaining senior management support, defining the project scope and objectives, estimating resource needs, and defining project timeframe.

Question ID: CISSP-2018-RA-01-2-115

Question: Which entity is ultimately responsible for approving the business continuity scope and plan?

A: Project manager
B: BCP team
C: Senior management
D: Department managers

Answer(s): C

Explanation: Senior management is ultimately responsible for approving the business continuity scope and plan. Although the other entities may be involved in the development of the business continuity scope and plan, they are not responsible for the approval.

Question ID: CISSP-2018-RA-01-2-116

Question: Your team has developed the business continuity scope and plan that will be presented to management for approval. You have been asked to provide a business case to prove the need for the scope and plan. Which of the following should you NOT give in this scenario?

A: Natural disasters
B: Utility disruption
C: Legal requirements
D: Competitive advantage

Answer(s): D

Explanation: Developing a business continuity scope and plan will NOT provide the organization with a competitive advantage. The business case for developing a business continuity scope and plan include natural disasters, utility disruptions, and legal requirements.

Question ID: CISSP-2018-RA-01-2-117

Question: Which agreements normally apply to personnel even after they are no longer employed by the organization?

A: NDAs
B: Noncompete clauses
C: Code of conduct
D: Ethics agreement
E: Statements a and b only
F: Statements b and c only
G: None of the statements

Answer(s): E

Explanation: Even after personnel are no longer employed by an organization, they must still abide by the NDA and the noncompete clauses that they signed. In most cases, the noncompete clause has an expiration date. They are no longer required to follow a code of conduct or ethics agreement after employment termination.

Question ID: CISSP-2018-RA-01-2-118

Question: Which agreements normally apply to personnel only while they are employed by the organization?

A: NDAs
B: Noncompete clauses
C: Code of conduct
D: Ethics agreement
E: Statements a and b only
F: Statements c and d only

G: None of the statements

Answer(s): F

Explanation: The code of conduct and ethics agreement normally apply to personnel only while they are employed by the organization.

Question ID: CISSP-2018-RA-01-2-119

Question: After accessing your organization and its security needs, you make several recommendations to management. Management decides to implement most of your recommendations. However, they feel that one of your recommendations is too expensive to implement. Management comes up with an alternative recommendation that is less expensive. This an example of which type of control?

A: Corrective
B: Deterrent
C: Preventive
D: Compensative

Answer(s): D

Explanation: The control that is recommended by management is a compensative control because it provides an alternative to another control. Compensative controls often do not provide the same level of protection as the alternative but are usually cheaper to implement.

Question ID: CISSP-2018-RA-01-2-120

Question: After accessing your organization and its security needs, you make several recommendations regarding security training for personnel. Management decides to adopt all the security training recommendations. Of which type of control are these recommendations an example?

A: Administrative
B: Technical
C: Physical
D: Recovery

Answer(s): A

Explanation: Security training is an example of an administrative control.

Question ID: CISSP-2018-RA-01-2-121

Question: As part of your company's comprehensive security program, the security auditor periodically reviews the audit logs to determine if any new controls need to be implemented. This an example of which type of control?

A: Administrative control
B: Technical control
C: Physical control
D: Detective control
E: Preventive control
F: Recovery control
G: Statements b and d only
H: Statements a and e only
I: Statements c and f only

Answer(s): G

Explanation: Audit logs are an example of a technical, detective control.

Question ID: CISSP-2018-RA-01-2-122

Question: Because security-in-depth has been adopted as a goal of your company, a security analyst was hired to complete a security audit. During the audit, the security analyst recommended that your company periodically create server images for storage at an offsite location. Of which type of controls are these images?

A: Administrative control
B: Technical control
C: Physical control
D: Corrective control
E: Preventive control
F: Recovery control
G: Statements b and d only
H: Statements a and e only
I: Statements c and f only

Answer(s): G

Explanation: Server images are corrective, technical controls.

Question ID: CISSP-2018-RA-01-2-123

Question: Because security-in-depth has been adopted as a goal of your company, a security

analyst was hired to complete a security audit. During the audit, the security analyst suggests that your company adopt a companywide security policy. Of which type of controls is this policy?

A: Administrative control
B: Technical control
C: Physical control
D: Corrective control
E: Preventive control
F: Recovery control
G: Statements b and d only
H: Statements a and e only
I: Statements c and f only

Answer(s): H

Explanation: Security policies are administrative, preventive controls.

Question ID: CISSP-2018-RA-01-2-124

Question: Because security-in-depth has been adopted as a goal of your company, a security analyst was hired to complete a security audit. During the audit, the security analyst suggests that your company's data center be protected by implementing biometrics. Of which type of controls is this data center protection?

A: Administrative control
B: Technical control
C: Physical control
D: Corrective control
E: Preventive control
F: Recovery control
G: Statements b and d only
H: Statements a and f only
I: Statements c and e only

Answer(s): I

Explanation: Biometrics are an example of a physical, preventive control.

Question ID: CISSP-2018-RA-01-2-125

Question: Because security-in-depth has been adopted as a goal of your company, a security analyst was hired to complete a security audit. During the audit, the security analyst suggests that your company implements job rotation in several departments. Of which type of controls is this

personnel policy?

A: Administrative control
B: Technical control
C: Physical control
D: Corrective control
E: Preventive control
F: Recovery control
G: Statements b and d only
H: Statements a and f only
I: Statements c and e only

Answer(s): A

Explanation: Job rotation is an administrative control. It is also considered to be a detective control, but this is not listed as an option.

Question ID: CISSP-2018-RA-01-2-126

Question: Which framework gives guidelines on how to develop and maintain an information security management system?

A: Zachman Framework
B: ISO/IEC 27000
C: NIST SP 800-53
D: ITIL

Answer(s): B

Explanation: ISO/IEC 27000 gives guidelines on how to develop and maintain an information security management system. Zachman Framework is an enterprise architecture framework. It is a two-dimensional classification system based on six communication questions (What, Where, When, Why, Who, and How) that intersect with different views (Planner, Owner, Designer, Builder, Subcontractor, and Actual System). NIST SP 800-53 is a security controls development framework. ITIL is a process management development standard.

Question ID: CISSP-2018-RA-01-2-127

Question: Which framework is an enterprise architecture framework that uses a two-dimensional classification system based on six communication questions (What, Where, When, Why, Who, and How) that intersect with different views (Planner, Owner, Designer, Builder, Subcontractor, and Actual System)?

A: Zachman Framework
B: ISO/IEC 27000
C: NIST SP 800-53
D: ITIL

Answer(s): A

Explanation: Zachman Framework is an enterprise architecture framework that uses a two-dimensional classification system based on six communication questions (What, Where, When, Why, Who, and How) that intersect with different views (Planner, Owner, Designer, Builder, Subcontractor, and Actual System). ISO/IEC 27000 gives guidelines on how to develop and maintain an information security management system. NIST SP 800-53 is a security controls development framework. ITIL is a process management development standard.

Question ID: CISSP-2018-RA-01-2-128

Question: Which of the following should be considered as part of any third-party governance?

A: On-site assessment
B: Policy review
C: Document exchange
D: Document review
E: Statements a, b, and c only
F: All the statements

Answer(s): F

Explanation: All of the listed options should be considered as part of any third-party governance.

Question ID: CISSP-2018-RA-01-2-129

Question: Which of the following is NOT included in the security awareness training provided to nonspecialized personnel?

A: Organizational security policies
B: Social engineering issues
C: Laws that affect the organization's security practices
D: Data classification

Answer(s): C

Explanation: Laws that affect the organization's security practices is NOT included in the

security awareness training provided to non-specialized personnel.

Question ID: CISSP-2018-RA-01-2-130

Question: Which of the following statements regarding security awareness training are FALSE?

A: The security awareness training should explain the organizational security policy.
B: The security awareness training should explain how the organizational security policy affects personnel and their roles in the organization.
C: The security awareness training should give the penalties for noncompliance with the organizational security policy.
D: The security awareness training should only be given to non-managerial personnel.
E: Statements a and d only
F: Statements b and d only
G: Statements c and d only

Answer(s): D

Explanation: The security awareness training should NOT only be given to nonmanagerial staff. Security awareness training is for all personnel at every level of the organization.

Question ID: CISSP-2018-RA-01-3-001

Question: Your organization implements hard drive encryption on a file server. Which security tenet will this cover?

A: Confidentiality
B: Integrity
C: Availability
D: Accountability

Answer(s): A

Explanation: Implementing hard drive encryption on a file server will cover the confidentiality tenet.

Question ID: CISSP-2018-RA-01-3-002

Question: The security administrator at your company suggests that auditing is configured on all servers. Management decides to make this part of the company's security policy. Which tenet will this cover?

A: Confidentiality

B: Integrity
C: Availability
D: Accountability

Answer(s): D

Explanation: Configuring auditing on all servers will cover the accountability tenet. Auditing is used to log certain actions that are performed by users. Administrators can then review these logs to provide user accountability.

Question ID: CISSP-2018-RA-01-3-004

Question: A company decides to implement a redundant network backbone. Which tenet will this cover?

A: Confidentiality
B: Integrity
C: Availability
D: Authentication

Answer(s): C

Explanation: Implementing a redundant network backbone will covers availability. If the first network backbone goes down, the redundant backbone will continue to function, ensuring that the network is still available.

Question ID: CISSP-2018-RA-01-3-005

Question: Which components act as limiting factors on an organization's security function?

A: Budget
B: Metrics
C: Resources
D: Skills and abilities
E: Statements a, b, and c only
F: All the statements

Answer(s): F

Explanation: All the listed components act as limiting factors on an organization's security function.

Question ID: CISSP-2018-RA-01-3-006

Question: Which group of users poses the greatest threat to an organization's security?

A: Hackers
B: Hactivists
C: Internal users
D: Guests

Answer(s): C

Explanation: Internal users pose the greatest threat to an organization's security.

Question ID: CISSP-2018-RA-01-3-007

Question: Which security model is a framework in addition to a methodology in that it prescribes the processes to follow to build and maintain the architecture?

A: SABSA
B: TOGAF
C: Zachman Framework
D: IOS/IEC 27000
E: COBiT

Answer(s): A

Explanation: The listed models are defined as follows: Zachman Framework: A two-dimensional model that intersects communication interrogatives (what, why, where, and so on) with various viewpoints (planner, owner, designer, and so on). Sherwood Applied Business Security Architecture (SABSA): It is a framework in addition to a methodology in that it prescribes the processes to follow to build and maintain the architecture. The Open Group Architecture Framework (TOGAF): Calls for an Architectural Development Method (ADM) that employs an iterative process that calls for individual requirements to be continuously monitored and updated as needed. ISO/IEC 27000-series: Establishes information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Control Objectives for Information and Related Technology (COBIT): A set of control objectives used as a framework for IT governance.

Question ID: CISSP-2018-RA-01-3-008

Question: Which security model is a two-dimensional model that intersects communication interrogatives with various viewpoints?

A: SABSA
B: TOGAF
C: Zachman Framework
D: IOS/IEC 27000
E: COBIT

Answer(s): C

Explanation: The listed models are defined as follows: Zachman Framework: A two-dimensional model that intersects communication interrogatives (what, why, where, and so on) with various viewpoints (planner, owner, designer, and so on). Sherwood Applied Business Security Architecture (SABSA): It is a framework in addition to a methodology in that it prescribes the processes to follow to build and maintain the architecture. The Open Group Architecture Framework (TOGAF): Calls for an Architectural Development Method (ADM) that employs an iterative process that calls for individual requirements to be continuously monitored and updated as needed. ISO/IEC 27000-series: Establishes information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Control Objectives for Information and Related Technology (COBIT): A set of control objectives used as a framework for IT governance.

Question ID: CISSP-2018-RA-01-3-009

Question: Which security model calls for an Architectural Development Method (ADM) that employs an iterative process?

A: SABSA
B: TOGAF
C: Zachman Framework
D: IOS/IEC 27000
E: COBIT

Answer(s): B

Explanation: The listed models are defined as follows: Zachman Framework: A two-dimensional model that intersects communication interrogatives (what, why, where, and so on) with various viewpoints (planner, owner, designer, and so on). Sherwood Applied Business Security Architecture (SABSA): It is a framework in addition to a methodology in that it prescribes the processes to follow to build and maintain the architecture. The Open Group Architecture Framework (TOGAF): Calls for an Architectural Development Method (ADM) that employs an iterative process that calls for individual requirements to be continuously monitored and updated as needed. ISO/IEC 27000-series: Establishes information security standards published jointly by the International Organization for Standardization (ISO) and the

International Electrotechnical Commission (IEC). Control Objectives for Information and Related Technology (COBIT): A set of control objectives used as a framework for IT governance.

Question ID: CISSP-2018-RA-01-3-010

Question: Which laws should be consulted to determine the types of employee monitoring that are permissible?

A: State
B: Local
C: County
D: Federal

Answer(s): A

Explanation: State law typically should guide the local monitoring practices.

Question ID: CISSP-2018-RA-01-3-011

Question: Which type of law grants the right to control either the distribution or the reproduction of a work?

A: Criminal law
B: Copyright law
C: Administrative law
D: Civil law

Answer(s): B

Explanation: The listed types of law are defined as follows: Civil law: Governs the payment of compensation and fines without sentencing the offenders to jail. Criminal law: Applies to offenders who violate government laws meant to protect the public. The common punishment in a criminal case is a jail sentence for the individual. Copyright law: Grants the right to control either the distribution or the reproduction of his work to an author. Administrative law: Ensures that the companies and individuals adhere to the regulatory standards prescribed by the government.

Question ID: CISSP-2018-RA-01-3-012

Question: What term describes risk that remains after implementing countermeasures?

A: Legal liability

B: Residual risk
C: Downstream liability
D: Total risk

Answer(s): B

Explanation: The listed terms are defined as follows: Legal liability: Extent of liability that exists for not exercising due care and diligence. Residual risk: Risk that remains after implementing countermeasures. Total risk: Risk that exists before implementing countermeasures. Downstream liability: Ensures that organizations working together under a contract are responsible for their information security management and the security controls deployed by each organization.

Question ID: CISSP-2018-RA-01-3-013

Question: Which type of law ensures that companies and individuals adhere to regulatory standards?

A: Criminal law
B: Copyright law
C: Administrative law
D: Civil law

Answer(s): C

Explanation: The listed types of law are defined as follows: Civil law: Governs the payment of compensation and fines without sentencing the offenders to jail. Criminal law: Applies to offenders who violate government laws meant to protect the public. The common punishment in a criminal case is a jail sentence for the individual. Copyright law: Grants the right to control either the distribution or the reproduction of his work to an author. Administrative law: Ensures that the companies and individuals adhere to the regulatory standards prescribed by the government.

Question ID: CISSP-2018-RA-01-3-014

Question: What concept ensures that organizations working together under a contract are responsible for their information security management and the security controls deployed by each organization?

A: Legal liability
B: Residual risk
C: Downstream liability
D: Total risk

Answer(s): C

Explanation: The listed terms are defined as follows: Legal liability: Extent of liability that exists for not exercising due care and diligence. Residual risk: Risk that remains after implementing countermeasures. Total risk: Risk that exists before implementing countermeasures. Downstream liability: Ensures that organizations working together under a contract are responsible for their information security management and the security controls deployed by each organization.

Question ID: CISSP-2018-RA-01-3-015

Question: Which legislation requires appropriate training of system users or owners where the systems house sensitive information?

A: Computer Security Act of 1987
B: Economic Espionage Act of 1996
C: Privacy Act of 1974
D: European Union Principles on Privacy

Answer(s): A

Explanation: The listed pieces of legislation follow: Privacy Act of 1974: Ensures that only authorized persons should have access to personal information and that personal records should be up to date and accurate. Computer Security Act of 1987: Requires the creation of computer security plans and the appropriate training of system users or owners where the systems house sensitive information. Economic Espionage Act of 1996: Provides a framework to deal with espionage attacks on corporations. According to the Act, all the assets of the organization, whether substantial or not, require protection. European Union Principles on Privacy: States that the data gathered for private individuals should be used only for the purpose for which it is collected.

Question ID: CISSP-2018-RA-01-3-016

Question: Which legislation affects financial institutions?

A: GLBA
B: CFAA
C: HIPAA
D: SOX

Answer(s): A

Explanation: The Gramm-Leach-Bliley Act (GLBA) of 1999 affects all financial institutions, including banks, loan companies, insurance companies, investment companies, and credit card providers.

Question ID: CISSP-2018-RA-01-3-017

Question: Which legislation states that the data gathered for private individuals should be used only for the purpose for which it is collected?

A: Computer Security Act of 1987
B: Economic Espionage Act of 1996
C: Privacy Act of 1974
D: European Union Principles on Privacy

Answer(s): D

Explanation: The listed pieces of legislation follow: Privacy Act of 1974: Ensures that only authorized persons should have access to personal information and that personal records should be up to date and accurate. Computer Security Act of 1987: Requires the creation of computer security plans and the appropriate training of system users or owners where the systems house sensitive information. Economic Espionage Act of 1996: Provides a framework to deal with espionage attacks on corporations. According to the Act, all the assets of the organization, whether substantial or not, require protection. European Union Principles on Privacy: States that the data gathered for private individuals should be used only for the purpose for which it is collected.

Question ID: CISSP-2018-RA-01-3-018

Question: Which of the following regulations applies to “protected computers”?

A: SOX
B: HIPAA
C: GLBA
D: Computer Fraud and Abuse Act

Answer(s): D

Explanation: The listed regulations are defined as follows: Sarbanes-Oxley (SOX) Act of 2002: Provides guidelines on accurately reporting corporate financial data to shareholders and the public Health Insurance Portability and Accountability Act (HIPAA): Was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient healthcare information without consent Gramm-Leach-Bliley Act (GLBA) of 1999: Was written to ensure that financial institutions develop privacy notices and allow their

customers to prevent the financial institutions from sharing information with third parties. Computer Fraud and Abuse Act: Affects any entities that might engage in hacking of "protected computers" as defined in the Act

Question ID: CISSP-2018-RA-01-3-019

Question: Which of the following was the first law written to require a formal computer security plan?

A: CFAA
B: ECPA
C: Federal Privacy Act of 1974
D: FISA
E: Computer Security Act of 1987

Answer(s): E

Explanation: The listed laws are defined as follows: Computer Fraud and Abuse Act (CFAA) of 1986: Affects any entities that may engage in hacking of "protected computers" as defined in the Act Federal Privacy Act of 1974: Affects any computer that contains records used by a federal agency Federal Intelligence Surveillance Act (FISA) of 1978: Affects law enforcement and intelligence agencies Electronic Communications Privacy Act (ECPA) of 1986: Extended government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer and prohibited access to stored electronic communications Computer Security Act of 1987: Was the first law written to require a formal computer security plan

Question ID: CISSP-2018-RA-01-3-020

Question: Which of the following laws provides guidelines to prevent sentencing disparities that existed across the United States?

A: Economic Espionage Act of 1996
B: Communications Assistance for Law Enforcement Act (CALEA) of 1994
C: Personal Information Protection and Electronic Documents Act (PIPEDA)
D: United States Federal Sentencing Guidelines of 1991
E: Federal Information Security Management Act (FISMA) of 2002
F: Payment Card Industry Data Security Standard (PCI DSS)

Answer(s): D

Explanation: The listed laws are defined as follows: United States Federal Sentencing Guidelines of 1991: Affects individuals and organizations convicted of felonies and serious (Class A) misdemeanors. It provides guidelines to prevent sentencing disparities that exist across

the United States. Communications Assistance for Law Enforcement Act (CALEA) of 1994: Requires telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities. Personal Information Protection and Electronic Documents Act (PIPEDA): Affects private sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada. Payment Card Industry Data Security Standard (PCI DSS): Affects any organizations that handle cardholder information for the major credit card companies. Federal Information Security Management Act (FISMA) of 2002: Affects every federal agency. It requires the federal agencies to develop, document, and implement an agency-wide information security program. Economic Espionage Act of 1996: Affects companies that have trade secrets and any individuals who plan to use encryption technology for criminal activities.

Question ID: CISSP-2018-RA-01-3-021

Question: As a security professional, you must adhere to the Code of Ethics of many organizations, including (ISC)2. If any guidelines within the different Code of Ethics contradict each other, which Code of Ethics should take precedence?

A: The Code of Ethics that you agreed to adhere to first
B: The Code of Ethics that you agreed to adhere to last
C: The most restrictive guidelines in the Code of Ethics
D: The least restrictive guidelines in the Code of Ethics

Answer(s): C

Explanation: The most restrictive guidelines in the Code of Ethics should take precedence if guidelines within the different Code of Ethics contradict each other.

Question ID: CISSP-2018-RA-01-3-022

Question: Which of the following is NOT a part of the (ISC)² Code of Ethics?

A: Act honorably and justly.
B: Work diligently to provide competent service.
C: Comply with the letter of the law.
D: Avoid conflicts of interest.

Answer(s): C

Explanation: Some actions may be legal but not ethical. The four canons of the (ISC)2 Code of Ethics are as follows: Protect society, the common good, necessary public trust and confidence, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally. Provide diligent

and competent service to principals. Advance and protect the profession.

Question ID: CISSP-2018-RA-01-3-023

Question: Which of the following organizations issues ethics related statements concerning the use of the Internet?

A: IEEE
B: IAB
C: IANA
D: CSIRT

Answer(s): B

Explanation: The Internet Architecture Board (IAB) is a coordinating committee for Internet design that issues ethics related statements concerning the use of the Internet.

Question ID: CISSP-2018-RA-01-3-024

Question: Which RFC is called Ethics and the Internet?

A: RFC 1087
B: RFC 2010
C: RFC 1589
D: RFC 1150

Answer(s): A

Explanation: RFC 1087 outlines concepts pertaining to what the IAB considers unethical and unacceptable.

Question ID: CISSP-2018-RA-01-3-025

Question: The (ISC)² Code of Ethics includes which of the following behaviors for a CISSP?

A: Behavioral
B: Physical
C: Control
D: Detection

Answer(s): A

Explanation: The (ISC)² Code of Ethics focuses on moral, ethical, and legal issues.

Question ID: CISSP-2018-RA-01-3-026

Question: What is the purpose of a baseline?

A: To provide the steps necessary to achieve security
B: To assess the security state
C: To provide all the detailed actions that personnel are required to follow
D: To provide recommended actions to carry out under certain conditions

Answer(s): B

Explanation: The purpose of a baselines is to assess the security state. Standards provide the steps necessary to achieve security. Procedures provide all the detailed actions that personnel are required to follow. Guidelines provide recommended actions to carry out under certain conditions.

Question ID: CISSP-2018-RA-01-3-027

Question: What is the purpose of procedures?

A: To provide the steps necessary to achieve security
B: To assess the security state
C: To provide all the detailed actions that personnel are required to follow
D: To provide recommended actions to carry out under certain conditions

Answer(s): C

Explanation: Procedures provide all the detailed actions that personnel are required to follow. Standards provide the steps necessary to achieve security. Baselines assess the security state. Guidelines provide recommended actions to carry out under certain conditions.

Question ID: CISSP-2018-RA-01-3-028

Question: What is the purpose of guidelines?

A: To provide the steps necessary to achieve security
B: To assess the security state
C: To provide all the detailed actions that personnel are required to follow
D: To provide recommended actions to carry out under certain conditions

Answer(s): D

Explanation: Guidelines provide recommended actions to carry out under certain conditions. Standards provide the steps necessary to achieve security. Baselines assess the security state. Procedures provide all the detailed actions that personnel are required to follow.

Question ID: CISSP-2018-RA-01-3-029

Question: What is the purpose of standards?

A: To provide the steps necessary to achieve security
B: To assess the security state
C: To provide all the detailed actions that personnel are required to follow
D: To provide recommended actions to carry out under certain conditions

Answer(s): A

Explanation: Standards provide the steps necessary to achieve security. Baselines assess the security state. Procedures provide all the detailed actions that personnel are required to follow. Guidelines provide recommended actions to carry out under certain conditions.

Question ID: CISSP-2018-RA-01-3-030

Question: Which of the following should be included as part of the initial stage when developing the business continuity scope and plan?

A: Define roles.
B: Implement controls.
C: Develop recovery strategies.
D: Test the plan.

Answer(s): A

Explanation: When developing the business continuity scope and plan, roles should be defined. In addition, goals should be defined, and management approval should be obtained. All the other steps should be completed only AFTER the business continuity scope and plan have been approved.

Question ID: CISSP-2018-RA-01-3-031

Question: Which of the following should you NOT consider while developing the business continuity scope?

A: Organizational policies
B: Laws

C: Risks
D: Industry standards

Answer(s): C

Explanation: You should NOT consider risks while developing the business continuity scope. Risks are usually explored during risk assessment as part of a business impact analysis (BIA). Developing the business continuity scope is the initial stage of providing a business continuity plan. As part of its development, you should consider organizational policies, laws, and industry standards.

Question ID: CISSP-2018-RA-01-3-032

Question: Who is responsible for establishing the priorities of the goals outlined in the business continuity scope?

A: BCP team
B: BCP project manager
C: Business units
D: Senior management

Answer(s): D

Explanation: Senior management is responsible for establishing the priorities of the goals outlined in the business continuity scope. After senior management has established the high-level priorities, other groups and individuals, including the BCP team, the BCP project management, and the business units' management and staff uses the high-level priorities to set up individual resource priorities.

Question ID: CISSP-2018-RA-01-3-033

Question: How often should an organization review the business continuity scope?

A: Monthly
B: Quarterly
C: Annually
D: When a significant change occurs in the organization
E: When a senior management member leaves the organization
F: Statements a and d only
G: Statements a, d, and e only
H: Statements c and d only
I: Statements c, d, and e only

Answer(s): H

Explanation: An organization should review the business continuity scope annually and whenever a significant change occurs in the organization.

Question ID: CISSP-2018-RA-01-3-034

Question: Which of the following is generally NOT performed as part of a background check?

A: Military record
B: Medical history
C: Immigration status check
D: Drug screening
E: Statements a and b only
F: Statements b and c only

Answer(s): B

Explanation: Medical history is generally NOT performed as part of a background check. All of the other options are valid as part of a background check.

Question ID: CISSP-2018-RA-01-3-035

Question: Which of the following passwords does NOT strengthen the security of passwords?

A: Require that passwords are changed every 90 days.
B: Require that passwords consist of eight characters.
C: Require that passwords consist of uppercase and lowercase letter, numerals, and symbols.
D: Require that passwords consist of dictionary words.

Answer(s): D

Explanation: Requiring that passwords consist of dictionary words does NOT strengthen the security of passwords.

Question ID: CISSP-2018-RA-01-3-036

Question: At which time should new personnel sign all agreements and contracts?

A: At termination
B: At hiring
C: At the annual employment anniversary
D: After completing the probation period

Answer(s): B

Explanation: New personnel should sign all agreements and contracts at hiring.

Question ID: CISSP-2018-RA-01-3-037

Question: At which time should personnel complete an exit interview?

A: At termination
B: At hiring
C: At the annual performance review
D: After completing the probation period

Answer(s): A

Explanation: Personnel should complete an exit interview at termination.

Question ID: CISSP-2018-RA-01-3-038

Question: On which personnel would an organization MOST likely need to obtain a credit report?

A: Human Resources personnel
B: Accounting personnel
C: Assembly line manager
D: IT personnel

Answer(s): B

Explanation: An organization would MOST likely need to obtain a credit report on accounting personnel or any other personnel that will handle cash or other financial transactions.

Question ID: CISSP-2018-RA-01-3-039

Question: Which framework is a security controls development framework?

A: Zachman Framework
B: ISO/IEC 27000
C: NIST SP 800-53
D: ITIL

Answer(s): C

Explanation: NIST SP 800-53 is a security controls development framework. Zachman Framework is an enterprise architecture framework that uses a two-dimensional classification system based on six communication questions (What, Where, When, Why, Who, and How) that intersect with different views (Planner, Owner, Designer, Builder, Subcontractor, and Actual System). ISO/IEC 27000 gives guidelines on how to develop and maintain an information security management system. ITIL is a process management development standard.

Question ID: CISSP-2018-RA-01-3-040

Question: Which framework is a process management development standard?

A: Zachman Framework
B: ISO/IEC 27000
C: NIST SP 800-53
D: ITIL

Answer(s): D

Explanation: ITIL is a process management development standard. Zachman Framework is an enterprise architecture framework that uses a two-dimensional classification system based on six communication questions (What, Where, When, Why, Who, and How) that intersect with different views (Planner, Owner, Designer, Builder, Subcontractor, and Actual System). ISO/IEC 27000 gives guidelines on how to develop and maintain an information security management system. NIST SP 800-53 is a security controls development framework.

Question ID: CISSP-2018-RA-01-3-041

Question: Which model or framework is a process improvement approach that addresses three areas of interest: development, services, and acquisitions?

A: CMMI
B: Six Sigma
C: CobiT
D: DoDAF

Answer(s): A

Explanation: Capability Maturity Model Integration (CMMI) is a process improvement approach that addresses three areas of interest: development, services, and acquisitions. Six Sigma includes the DMAIC and DMADV methodologies. CobiT is a security controls development framework that uses a process model to subdivide IT into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and

Evaluate (ME). Department of Defense Architecture Framework (DoDAF) is an architecture framework that organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV).

Question ID: CISSP-2018-RA-01-3-042

Question: Which model or framework includes the DMAIC and DMADV methodologies?

A: CMMI
B: Six Sigma
C: CobiT
D: DoDAF

Answer(s): B

Explanation: Six Sigma includes the DMAIC and DMADV methodologies. Capability Maturity Model Integration (CMMI) is a process improvement approach that addresses three areas of interest: development, services, and acquisitions. CobiT is a security controls development framework that uses a process model to subdivide IT into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). Department of Defense Architecture Framework (DoDAF) is an architecture framework that organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV).

Question ID: CISSP-2018-RA-01-3-043

Question: Which model or framework uses a process model to subdivide IT into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME)?

A: CMMI
B: Six Sigma
C: CobiT
D: DoDAF

Answer(s): C

Explanation: CobiT is a security controls development framework that uses a process model to subdivide IT into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). Capability Maturity Model Integration (CMMI) is a process improvement approach that addresses three areas of interest: development, services, and acquisitions. Six Sigma includes the DMAIC and DMADV methodologies. Department of Defense Architecture Framework (DoDAF) is an architecture framework that

organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV).

Question ID: CISSP-2018-RA-01-3-044

Question: Which model or framework organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV)?

A: CMMI
B: Six Sigma
C: CobiT
D: DoDAF

Answer(s): D

Explanation: Department of Defense Architecture Framework (DoDAF) is an architecture framework that organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV). Capability Maturity Model Integration (CMMI) is a process improvement approach that addresses three areas of interest: development, services, and acquisitions. Six Sigma includes the DMAIC and DMADV methodologies. CobiT is a security controls development framework that uses a process model to subdivide IT into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME).

Question ID: CISSP-2018-RA-01-3-045

Question: Which framework is designed for use with the military?

A: DoDAF
B: MODAF
C: Zachman
D: TOGAF
E: Statements a and b only
F: All the statements

Answer(s): E

Explanation: U.S. Department of Defense Architecture Framework (DoDAF) and British Ministry of Defence Architecture Framework (MODAF) are designed for use with the military.

Question ID: CISSP-2018-RA-01-3-046

Question: Which enterprise architecture framework is based on four inter-related domains:

technology, applications, data, and business?

A: TOGAF
B: DoDAF
C: MODAF
D: SABSA

Answer(s): A

Explanation: The Open Group Architecture Framework (TOGAF) is an enterprise architecture framework that is based on four inter-related domains: technology, applications, data, and business. DoDAF is an architecture framework that organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV). British Ministry of Defence Architecture Framework (MODAF) is an architecture framework that divides information into seven viewpoints: strategic viewpoint (StV), operational viewpoint (OV), service-oriented viewpoint (SOV), systems viewpoint (SV), acquisition viewpoint (AcV), technical viewpoint (TV), and all viewpoint (AV). Sherwood Applied Business Security Architecture (SABSA) is an enterprise security architecture framework that is similar to the Zachman framework. It uses the six communication questions (What, Where, When, Why, Who, and How) that intersect with six layers (operational, component, physical, logical, conceptual, and contextual).

Question ID: CISSP-2018-RA-01-3-047

Question: Which enterprise architecture 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: TOGAF
B: DoDAF
C: MODAF
D: SABSA

Answer(s): D

Explanation: Sherwood Applied Business Security Architecture (SABSA) is an enterprise security architecture framework that uses the six communication questions (What, Where, When, Why, Who, and How) that intersect with six layers (operational, component, physical, logical, conceptual, and contextual). The Open Group Architecture Framework (TOGAF) is an enterprise architecture framework that is based on four inter-related domains: technology, applications, data, and business. DoDAF is an architecture framework that organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV). British Ministry of Defence Architecture Framework (MODAF) is an architecture

framework that divides information into seven viewpoints: strategic viewpoint (StV), operational viewpoint (OV), service-oriented viewpoint (SOV), systems viewpoint (SV), acquisition viewpoint (AcV), technical viewpoint (TV), and all viewpoint (AV).

Question ID: CISSP-2018-RA-01-3-048

Question: Which enterprise architecture framework organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV)?

A: TOGAF
B: DoDAF
C: MODAF
D: SABSA

Answer(s): B

Explanation: DoDAF is an architecture framework that organizes a set of products under four views: operational view (OV), system view (SV), technical standards view (TV), and all view (AV). The Open Group Architecture Framework (TOGAF) is an enterprise architecture framework that is based on four inter-related domains: technology, applications, data, and business. British Ministry of Defence Architecture Framework (MODAF) is an architecture framework that divides information into seven viewpoints: strategic viewpoint (StV), operational viewpoint (OV), service-oriented viewpoint (SOV), systems viewpoint (SV), acquisition viewpoint (AcV), technical viewpoint (TV), and all viewpoint (AV). Sherwood Applied Business Security Architecture (SABSA) is an enterprise security architecture framework that uses the six communication questions (What, Where, When, Why, Who, and How) that intersect with six layers (operational, component, physical, logical, conceptual, and contextual).

Question ID: CISSP-2018-RA-01-3-049

Question: Your company has decided to hire a third party to assess the organization's security issues. The personnel of this third party will need access to organizational assets both locally and remotely. What is the first step in properly establishing this relationship?

A: Perform a risk assessment on the third party's network.
B: Establish a written security policy with the third party.
C: Provide access to internal resources for the third-party personnel.
D: Audit the third party's access to internal resources.

Answer(s): A

Explanation: The steps in properly establishing a relationship with a third party when the third

party will need access to organizational assets both remotely and locally are as follows: 1. Perform a risk assessment on the third party's network. 2. Establish a written security policy with the third party. 3. Provide access to internal resources for the third-party personnel. 4. Audit the third party's access to internal resources.

Question ID: CISSP-2018-RA-01-3-050

Question: Why is it important to perform a risk assessment on a third party that will be remotely accessing internal resources?

A: To determine the level of access needed by the third party
B: To determine third party compliance with organizational security policies and standards
C: To determine if appropriate and inappropriate actions are being carried out by third-party personnel
D: To document the guidelines that the third party will follow

Answer(s): B

Explanation: It is important to perform a risk assessment on a third party to determine third-party compliance with organizational security policies and standards.

Question ID: CISSP-2018-RA-01-3-051

Question: A third party will be accessing your organization's compliance to ISO/IEC guidelines for auditing. Which ISO/IEC 27000 Series standard should you reference?

A: 27007
B: 27005
C: 27033
D: 27034

Answer(s): A

Explanation: You should reference ISO/IEC 27007 because it addresses auditing. ISO/IEC 27005 addresses risk management. ISO/IEC 27033 addresses network security. ISO/IEC 27034 addresses application security.

Question ID: CISSP-2018-RA-01-3-052

Question: A third party will be accessing your organization's compliance to ISO/IEC guidelines for risk management. Which ISO/IEC 27000 Series standard should you reference?

A: 27007

B: 27005
C: 27033
D: 27034

Answer(s): B

Explanation: You should reference ISO/IEC 27005 because it addresses risk management. ISO/IEC 27007 addresses auditing. ISO/IEC 27033 addresses network security. ISO/IEC 27034 addresses application security.

Question ID: CISSP-2018-RA-01-3-053

Question: A third party will be accessing your organization's compliance to ISO/IEC guidelines for network security. Which ISO/IEC 27000 Series standard should you reference?

A: 27007
B: 27005
C: 27033
D: 27034

Answer(s): C

Explanation: You should reference ISO/IEC 27033 because it addresses network security. ISO/IEC 27007 addresses auditing. ISO/IEC 27005 addresses risk management. ISO/IEC 27034 addresses application security.

Question ID: CISSP-2018-RA-01-3-054

Question: A third party will be accessing your organization's compliance to ISO/IEC guidelines for application security. Which ISO/IEC 27000 Series standard should you reference?

A: 27007
B: 27005
C: 27033
D: 27034

Answer(s): D

Explanation: You should reference ISO/IEC 27034 because it addresses application security. ISO/IEC 27007 addresses auditing. ISO/IEC 27005 addresses risk management. ISO/IEC 27033 addresses network security.

Question ID: CISSP-2018-RA-01-3-055

Question: You work for a telecommunications company that must comply with ISO/IEC standards. Which specific ISO/IEC 27000 Series standard should you reference for your industry?

A: 27011
B: 27015
C: 27037
D: 27799

Answer(s): A

Explanation: You should reference ISO/IEC 27011 because it addresses telecommunications organization guidelines. ISO/IEC 27015 addresses financial organization guidelines. ISO/IEC 27037 addresses digital evidence guidelines. ISO/IEC 27799 addresses health organization guidelines.

Question ID: CISSP-2018-RA-01-3-056

Question: You work for a financial organization that must comply with ISO/IEC standards. Which specific ISO/IEC 27000 Series standard should you reference for your industry?

A: 27011
B: 27015
C: 27037
D: 27799

Answer(s): B

Explanation: You should reference ISO/IEC 27015 because it addresses financial organization guidelines. ISO/IEC 27011 addresses telecommunications organization guidelines. ISO/IEC 27037 addresses digital evidence guidelines. ISO/IEC 27799 addresses health organization guidelines.

Question ID: CISSP-2018-RA-01-3-057

Question: You work for a financial organization that must comply with ISO/IEC standards for digital evidence identification, collection, acquisition, and preservation. Which specific ISO/IEC 27000 Series standard should you reference for your industry?

A: 27011
B: 27015
C: 27037

D: 27799

Answer(s): C

Explanation: You should reference ISO/IEC 27037 because it addresses digital evidence guidelines. ISO/IEC 27011 addresses telecommunications organization guidelines. ISO/IEC 27015 addresses financial organization guidelines. ISO/IEC 27799 addresses health organization guidelines.

Question ID: CISSP-2018-RA-01-3-058

Question: You work for a healthcare organization that must comply with ISO/IEC standards. Which specific ISO/IEC 27000 Series standard should you reference for your industry?

A: 27011
B: 27015
C: 27037
D: 27799

Answer(s): D

Explanation: You should reference ISO/IEC 27799 because it addresses health organization guidelines. ISO/IEC 27011 addresses telecommunications organization guidelines. ISO/IEC 27015 addresses financial organization guidelines. ISO/IEC 27037 addresses digital evidence guidelines.

Question ID: CISSP-2018-RA-01-3-059

Question: During a recent security audit, you discovered that the appropriate security patches have not been applied to an application. A hacker recently discovered this issue and, as a result, breached your network. You immediately update the application with all the latest security patches. Which aspect of this scenario is a control?

A: The update you performed
B: The audit you performed
C: The issue you discovered
D: The attack that occurred

Answer(s): A

Explanation: The update that you performed is a control. A control is a countermeasure that is put into place to reduce risk. The issue that you discovered is a vulnerability. Risk is the likelihood that a threat agent would exploit a vulnerability. The threat agent in this scenario is the

hacker. The exposure is the attack that occurred. If the attack had not been carried out, it would be deemed only a threat.

Question ID: CISSP-2018-RA-01-3-060

Question: During a recent security audit, you discovered that the appropriate security patches have not been applied to an application. A hacker recently discovered this issue and, as a result, breached your network. You immediately update the application with all the latest security patches. Which aspect of this scenario is a vulnerability?

A: The update you performed
B: The audit you performed
C: The issue you discovered
D: The attack that occurred

Answer(s): C

Explanation: The issue that you discovered is a vulnerability. The update that you performed is a control. A control is a countermeasure that is put into place to reduce risk. Risk is the likelihood that a threat agent would exploit a vulnerability. The threat agent in this scenario is the hacker. The exposure is the attack that occurred. If the attack had not been carried out, it would be deemed only a threat.

Question ID: CISSP-2018-RA-01-3-061

Question: What should you identify first as part of any risk assessment as part of NIST SP 800-30?

A: Assets and their value
B: Threats
C: Vulnerabilities
D: Likelihood

Answer(s): A

Explanation: SP 800-30 gives the following steps for a risk assessment: 1. Identify the assets and their value. 2. Identify threats. 3. Identify vulnerabilities. 4. Determine likelihood. 5. Identify impact. 6. Determine risk as a combination of likelihood and impact.

Question ID: CISSP-2018-RA-01-3-062

Question: What should you identify last as part of any risk assessment as part of NIST SP 800-30?

A: Assets and their value
B: Risk
C: Vulnerabilities
D: Likelihood

Answer(s): B

Explanation: SP 800-30 gives the following steps for a risk assessment: 1. Identify the assets and their value. 2. Identify threats. 3. Identify vulnerabilities. 4. Determine likelihood. 5. Identify impact. 6. Determine risk as a combination of likelihood and impact.

Question ID: CISSP-2018-RA-01-3-063

Question: What should you identify immediately after the threats and vulnerabilities are determined during a risk assessment as part of NIST SP 800-30?

A: Assets and their value
B: Risk
C: Likelihood
D: Impact

Answer(s): C

Explanation: SP 800-30 gives the following steps for a risk assessment: 1. Identify the assets and their value. 2. Identify threats. 3. Identify vulnerabilities. 4. Determine likelihood. 5. Identify impact. 6. Determine risk as a combination of likelihood and impact.

Question ID: CISSP-2018-RA-01-3-064

Question: Your organization has applied for approval by an industry governing agency. As part of this process, a third party will be reviewing all the policies and procedures that you have in place. What is the BEST description of the purpose of this review?

A: To document inaccuracies
B: To document performance metrics
C: To document service levels
D: To document compliance or noncompliance

Answer(s): D

Explanation: The best description of the purpose of reviewing all the policies and procedures that you have in place is to document compliance or noncompliance with the agency's standards.

Question ID: CISSP-2018-RA-01-3-065

Question: What is the most cost-effective way to enrich a security awareness program?

A: List penalties for noncompliance.
B: Create an award or recognition program.
C: Add an educational component.
D: Implement a security incident reporting mechanism.

Answer(s): B

Explanation: The most cost-effective way to enrich a security awareness program is to create an award or recognition program.

Question ID: CISSP-2018-RA-01-4-001

Question: A company has a virtual private network (VPN) that employees use to remotely access company resources. The security administrator decides to mandate the use of IPSec on the VPN. Which tenet will this cover?

A: Confidentiality
B: Integrity
C: Availability
D: Authentication

Answer(s): A

Explanation: Mandating the use of IPsec on the VPN will cover the confidentiality tenet. IPSec will encrypt data as it passes over the public network.

Question ID: CISSP-2018-RA-01-4-002

Question: A department manager requests that a RAID-5 array be implemented on a file server that contains data that is crucial to the department. Which tenet will this cover?

A: Confidentiality
B: Integrity
C: Availability
D: Authentication

Answer(s): C

Explanation: Implementing a RAID-5 array on a file server will cover the availability tenet. A RAID array is a group of independent hard drives that are configured to work together and provide fault tolerance if one drive in the array fails.

Question ID: CISSP-2018-RA-01-4-003

Question: Recently, a hacker used a social engineering attack to discover the passwords of several users. Which security tenet was compromised as a result of this attack?

A: Confidentiality
B: Integrity
C: Availability
D: Authentication

Answer(s): A

Explanation: Confidentiality was compromised as a result of this attack. User passwords should be considered confidential information.

Question ID: CISSP-2018-RA-01-4-004

Question: Recently, hackers successfully carried out a denial of service (DoS) attack against your company's database. Which security tenet was compromised during this attack?

A: Confidentiality
B: Integrity
C: Availability
D: Authentication

Answer(s): C

Explanation: Availability was compromised during this attack. A DoS attack will cause the device to be unavailable to legitimate users because the device is bombarded with connections.

Question ID: CISSP-2018-RA-01-4-005

Question: Several systems on your network have been infected with a virus. Which security tenet was compromised as a result of this infection?

A: Confidentiality
B: Integrity
C: Availability
D: Authentication

Answer(s): B

Explanation: Integrity was compromised during this infection.

Question ID: CISSP-2018-RA-01-4-006

Question: Which security model establishes information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)?

A: SABSA
B: TOGAF
C: Zachman Framework
D: IOS/IEC 27000
E: COBIT

Answer(s): D

Explanation: The listed models are defined as follows: Zachman Framework: A two-dimensional model that intersects communication interrogatives (what, why, where, and so on) with various viewpoints (planner, owner, designer, and so on). Sherwood Applied Business Security Architecture (SABSA): It is a framework in addition to a methodology in that it prescribes the processes to follow to build and maintain the architecture. The Open Group Architecture Framework (TOGAF): Calls for an Architectural Development Method (ADM) that employs an iterative process that calls for individual requirements to be continuously monitored and updated as needed. ISO/IEC 27000-series: Establishes information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Control Objectives for Information and Related Technology (COBIT): A set of control objectives used as a framework for IT governance.

Question ID: CISSP-2018-RA-01-4-007

Question: Which security model is a set of control objectives used as a framework for IT governance?

A: SABSA
B: TOGAF
C: Zachman Framework
D: IOS/IEC 27000
E: COBIT

Answer(s): E

Explanation: The listed models are defined as follows: Zachman Framework: A two-dimensional model that intersects communication interrogatives (what, why, where, and so on) with various viewpoints (planner, owner, designer, and so on). Sherwood Applied Business Security Architecture (SABSA): It is a framework in addition to a methodology in that it prescribes the processes to follow to build and maintain the architecture. The Open Group Architecture Framework (TOGAF): Calls for an Architectural Development Method (ADM) that employs an iterative process that calls for individual requirements to be continuously monitored and updated as needed. ISO/IEC 27000-series: Establishes information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Control Objectives for Information and Related Technology (COBIT): A set of control objectives used as a framework for IT governance.

Question ID: CISSP-2018-RA-01-4-008

Question: When an organization has taken the necessary steps to protect the organization, its resources, and personnel, it has applied which security principle?

A: Due diligence
B: Due care
C: Job rotation
D: Separation of duties

Answer(s): B

Explanation: Examples of the listed concepts are as follows: Separation of duties: . Prescribes that sensitive operations be divided among multiple users so that no one user has the rights and access to carry out the operation alone. Due diligence: Has been applied when you evaluate information to identify vulnerabilities, threats, and issues related to risk. Due care: Has been applied when an organization has taken the necessary steps to protect the organization, its resources, and personnel. Job rotation: Is in effect when more than one person completes the tasks of a single position within the organization.

Question ID: CISSP-2018-RA-01-4-009

Question: Which of the following concepts indicates that an organization properly investigated?

A: Chain of custody
B: Due diligence
C: Due care
D: Liability

Answer(s): B

Explanation: The listed terms are defined as follows: Chain of custody: Refers to strict and organized formal procedures in accordance with the law and the legal regulations governing the collection, analysis, and preservation of the evidence before the evidence is produced in a court of law Due diligence: Indicates that an organization properly investigated any identified weaknesses and vulnerabilities Due care: Indicates an organization took all proper security measures and took active measures to prevent security breaches Liability: Describes an organization's responsibility when a security breach occurs

Question ID: CISSP-2018-RA-01-4-010

Question: Who is ultimately responsible for the protection of private employee data on systems?

A: IT department
B: User
C: Manager
D: Security auditor

Answer(s): B

Explanation: Ultimately when a user puts personal information on a company system, he is responsible for its protection.

Question ID: CISSP-2018-RA-01-4-011

Question: Which of the following laws affect any entities that may engage in hacking of “protected computers”?

A: CFAA
B: ECPA
C: Federal Privacy Act of 1974
D: FISA
E: Computer Security Act of 1987

Answer(s): A

Explanation: The listed laws are defined as follows: Computer Fraud and Abuse Act (CFAA) of 1986: Affects any entities that may engage in hacking of “protected computers” as defined in the Act Federal Privacy Act of 1974: Affects any computer that contains records used by a federal agency Federal Intelligence Surveillance Act (FISA) of 1978: Affects law enforcement and intelligence agencies Electronic Communications Privacy Act (ECPA) of 1986: Extended

government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer and prohibited access to stored electronic communications Computer Security Act of 1987: Was the first law written to require a formal computer security plan

Question ID: CISSP-2018-RA-01-4-012

Question: Which of the following laws affects companies that have trade secrets?

A: Economic Espionage Act of 1996
B: Communications Assistance for Law Enforcement Act (CALEA) of 1994
C: Personal Information Protection and Electronic Documents Act (PIPEDA)
D: United States Federal Sentencing Guidelines of 1991
E: Federal Information Security Management Act (FISMA) of 2002
F: Payment Card Industry Data Security Standard (PCI DSS)

Answer(s): A

Explanation: The listed laws are defined as follows: United States Federal Sentencing Guidelines of 1991: Affects individuals and organizations convicted of felonies and serious (Class A) misdemeanors. It provides guidelines to prevent sentencing disparities that exist across the United States. Communications Assistance for Law Enforcement Act (CALEA) of 1994: Requires telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities. Personal Information Protection and Electronic Documents Act (PIPEDA): Affects private sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada. Payment Card Industry Data Security Standard (PCI DSS): Affects any organizations that handle cardholder information for the major credit card companies. Federal Information Security Management Act (FISMA) of 2002: Affects every federal agency. It requires the federal agencies to develop, document, and implement an agency-wide information security program. Economic Espionage Act of 1996: Affects companies that have trade secrets and any individuals who plan to use encryption technology for criminal activities.

Question ID: CISSP-2018-RA-01-4-013

Question: Which of the following laws extended government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer?

A: CFAA
B: ECPA
C: Federal Privacy Act of 1974
D: FISA
E: Computer Security Act of 1987

Answer(s): B

Explanation: The listed laws are defined as follows: Computer Fraud and Abuse Act (CFAA) of 1986: Affects any entities that may engage in hacking of "protected computers" as defined in the Act Federal Privacy Act of 1974: Affects any computer that contains records used by a federal agency Federal Intelligence Surveillance Act (FISA) of 1978: Affects law enforcement and intelligence agencies Electronic Communications Privacy Act (ECPA) of 1986: Extended government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer and prohibited access to stored electronic communications Computer Security Act of 1987: Was the first law written to require a formal computer security plan

Question ID: CISSP-2018-RA-01-4-014

Question: Which of the following laws requires federal agencies to develop, document, and implement an agency-wide information security program?

A: Economic Espionage Act of 1996
B: Communications Assistance for Law Enforcement Act (CALEA) of 1994
C: Personal Information Protection and Electronic Documents Act (PIPEDA)
D: United States Federal Sentencing Guidelines of 1991
E: Federal Information Security Management Act (FISMA) of 2002
F: Payment Card Industry Data Security Standard (PCI DSS)

Answer(s): E

Explanation: The listed laws are defined as follows: United States Federal Sentencing Guidelines of 1991: Affects individuals and organizations convicted of felonies and serious (Class A) misdemeanors. It provides guidelines to prevent sentencing disparities that exist across the United States. Communications Assistance for Law Enforcement Act (CALEA) of 1994: Requires telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities. Personal Information Protection and Electronic Documents Act (PIPEDA): Affects private sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada. Payment Card Industry Data Security Standard (PCI DSS): Affects any organizations that handle cardholder information for the major credit card companies. Federal Information Security Management Act (FISMA) of 2002: Affects every federal agency. It requires the federal agencies to develop, document, and implement an agency-wide information security program. Economic Espionage Act of 1996: Affects companies that have trade secrets and any individuals who plan to use encryption technology for criminal activities.

Question ID: CISSP-2018-RA-01-4-015

Question: Which of the following laws give procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers"?

A: CFAA
B: ECPA
C: Federal Privacy Act of 1974
D: FISA
E: Computer Security Act of 1987

Answer(s): D

Explanation: The listed laws are defined as follows: Computer Fraud and Abuse Act (CFAA) of 1986: Affects any entities that may engage in hacking of “protected computers” as defined in the Act Federal Privacy Act of 1974: Affects any computer that contains records used by a federal agency Federal Intelligence Surveillance Act (FISA) of 1978: Affects law enforcement and intelligence agencies Electronic Communications Privacy Act (ECPA) of 1986: Extended government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer and prohibited access to stored electronic communications Computer Security Act of 1987: Was the first law written to require a formal computer security plan

Question ID: CISSP-2018-RA-01-4-016

Question: Which of the following laws requires telecommunications carriers to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities?

A: Economic Espionage Act of 1996
B: Communications Assistance for Law Enforcement Act (CALEA) of 1994
C: Personal Information Protection and Electronic Documents Act (PIPEDA)
D: United States Federal Sentencing Guidelines of 1991
E: Federal Information Security Management Act (FISMA) of 2002
F: Payment Card Industry Data Security Standard (PCI DSS)

Answer(s): B

Explanation: The listed laws are defined as follows: United States Federal Sentencing Guidelines of 1991: Affects individuals and organizations convicted of felonies and serious (Class A) misdemeanors. It provides guidelines to prevent sentencing disparities that exist across the United States. Communications Assistance for Law Enforcement Act (CALEA) of 1994: Requires telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have built-in

surveillance capabilities. Personal Information Protection and Electronic Documents Act (PIPEDA): Affects private sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada. Payment Card Industry Data Security Standard (PCI DSS): Affects any organizations that handle cardholder information for the major credit card companies. Federal Information Security Management Act (FISMA) of 2002: Affects every federal agency. It requires the federal agencies to develop, document, and implement an agency-wide information security program. Economic Espionage Act of 1996: Affects companies that have trade secrets and any individuals who plan to use encryption technology for criminal activities.

Question ID: CISSP-2018-RA-01-4-017

Question: Which of the following laws affect any computer that contains records used by a federal agency?

A: CFAA
B: ECPA
C: Federal Privacy Act of 1974
D: FISA
E: Computer Security Act of 1987

Answer(s): C

Explanation: The listed laws are defined as follows: Computer Fraud and Abuse Act (CFAA) of 1986: Affects any entities that may engage in hacking of "protected computers" as defined in the Act Federal Privacy Act of 1974: Affects any computer that contains records used by a federal agency Federal Intelligence Surveillance Act (FISA) of 1978: Affects law enforcement and intelligence agencies Electronic Communications Privacy Act (ECPA) of 1986: Extended government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer and prohibited access to stored electronic communications Computer Security Act of 1987: Was the first law written to require a formal computer security plan

Question ID: CISSP-2018-RA-01-4-018

Question: Which of the following regulations was written to prevent medical organizations from sharing patient healthcare information without consent?

A: SOX
B: HIPAA
C: GLBA
D: Base II

Answer(s): B

Explanation: The listed regulations are defined as follows: Sarbanes-Oxley (SOX) Act of 2002: Provides guidelines on accurately reporting corporate financial data to shareholders and the public Health Insurance Portability and Accountability Act (HIPAA): Was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient healthcare information without consent Gramm-Leach-Bliley Act (GLBA) of 1999: Was written to ensure that financial institutions develop privacy notices and allow their customers to prevent the financial institutions from sharing information with third parties. Computer Fraud and Abuse Act: Affects any entities that might engage in hacking of "protected computers" as defined in the Act

Question ID: CISSP-2018-RA-01-4-019

Question: Which of the following laws affects private sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada?

A: Economic Espionage Act of 1996
B: Communications Assistance for Law Enforcement Act (CALEA) of 1994
C: Personal Information Protection and Electronic Documents Act (PIPEDA)
D: United States Federal Sentencing Guidelines of 1991
E: Federal Information Security Management Act (FISMA) of 2002
F: Payment Card Industry Data Security Standard (PCI DSS)

Answer(s): C

Explanation: The listed laws are defined as follows: United States Federal Sentencing Guidelines of 1991: Affects individuals and organizations convicted of felonies and serious (Class A) misdemeanors. It provides guidelines to prevent sentencing disparities that exist across the United States. Communications Assistance for Law Enforcement Act (CALEA) of 1994: Requires telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities. Personal Information Protection and Electronic Documents Act (PIPEDA): Affects private sector organizations that collect, use, and disclose personal information in the course of commercial business in Canada. Payment Card Industry Data Security Standard (PCI DSS): Affects any organizations that handle cardholder information for the major credit card companies. Federal Information Security Management Act (FISMA) of 2002: Affects every federal agency. It requires the federal agencies to develop, document, and implement an agency-wide information security program. Economic Espionage Act of 1996: Affects companies that have trade secrets and any individuals who plan to use encryption technology for criminal activities.

Question ID: CISSP-2018-RA-01-4-020

Question: Which of the following regulations is built on three main pillars: minimum capital requirements, supervision, and market discipline?

A: SOX
B: HIPAA
C: GLBA
D: Base II

Answer(s): D

Explanation: The listed regulations are defined as follows: Sarbanes-Oxley (SOX) Act of 2002: Provides guidelines on accurately reporting corporate financial data to shareholders and the public Health Insurance Portability and Accountability Act (HIPAA): Was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient healthcare information without consent Gramm-Leach-Bliley Act (GLBA) of 1999: Was written to ensure that financial institutions develop privacy notices and allow their customers to prevent the financial institutions from sharing information with third parties. Computer Fraud and Abuse Act: Affects any entities that might engage in hacking of "protected computers" as defined in the Act

Question ID: CISSP-2018-RA-01-4-021

Question: In which document is the phrase "Observe and abide by all contracts" found?

A: (ISC)² Code of Ethics
B: CEI commandments
C: RFC 1087
D: CIAC guidelines

Answer(s): A

Explanation: Among the phrases found in the (ISC)² Code of Ethics are "Observe and abide by all contracts" and "Discourage unsafe practices."

Question ID: CISSP-2018-RA-01-4-022

Question: Which type of engineering is considered unethical?

A: Inverse
B: Compound
C: Reverse
D: Source

Answer(s): C

Explanation: Reverse engineering, done in the hopes of understanding the intricate details of software functionality is considered unethical.