PassQueen
a.k.a dumpsqueen.com

ASIS - Certified Protection Professional (CPP) Exam

ASIS ASIS-CPP

Version Demo

Total Demo Questions: 96

Total Premium Questions: 965

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Principles and Practices	140
Topic 2, Business Principles and Practices	80
Topic 3, Investigations	191
Topic 4, Personnel Security	161
Topic 5, Physical Security	175
Topic 6, Information Security	93
Topic 7, Crisis Management	125
Total	965

QUESTION NO: 1

All policies and procedures for drug testing should be:

A. require mandatory testing of all managers.

B. applied on an " as needed " basis.

C. separate from any collective bargaining agreement.

D. administered consistently.

ANSWER: D

Explanation:

“Administered consistently” is correct because a workplace drug-testing program must apply its stated standards, selection methods, testing procedures, and consequences uniformly to similarly situated personnel. Consistent administration supports procedural fairness, helps demonstrate that testing decisions are based on established job-related criteria rather than individual bias, and makes the program more defensible if challenged. A protection professional should ensure that the written program identifies who may be tested, under what circumstances testing occurs, how specimens and results are handled confidentially, and how positive results or refusals are addressed. The organization must then implement those provisions reliably while complying with applicable law, privacy requirements, and any governing labor agreement. The U.S. Equal Employment Opportunity Commission notes that drug tests are not medical examinations under the Americans with Disabilities Act, but employment testing practices remain subject to nondiscrimination obligations and other applicable requirements. The Substance Abuse and Mental Health Services Administration also publishes mandatory testing guidelines that emphasize standardized collection, custody, laboratory, and review processes. These principles reinforce that consistency is fundamental to a credible, fair, and legally sound drug-testing policy. See the EEOC guidance on the ADA and employment rights and SAMHSA statutes, regulations, and testing guidelines.

QUESTION NO: 2

Individuals who find integrity tests offensive are:

A. Usually found to have a violent criminal past

B. Sensitive individuals who do not like to take tests

C. Twice as likely to be involved in some type of drug abuse behavior

D. Twice as likely to admit to criminal activity or drug abuse

E. None of the above

ANSWER: D

Explanation:

Twice as likely to admit to criminal activity or drug abuse is correct. In the personnel-selection research underlying overt integrity tests, a strongly negative or offended reaction to the test is itself associated with greater self-reported involvement in counterproductive behaviors, including criminal conduct and substance misuse. The point is not that feeling offended proves misconduct in an individual case; rather, it is a group-level empirical finding used to describe the response patterns observed in integrity-test validation research. Overt integrity measures commonly ask directly about attitudes toward theft, rule compliance, prior dishonest conduct, and drug use. Candidates who object strongly to these questions have, in the cited finding, been about twice as likely to acknowledge criminal activity or drug-abuse behavior when compared with candidates who do not express that level of offense. For protection professionals, this supports using validated integrity assessments only as one structured component of a lawful, job-related selection process, with consistent administration and appropriate interpretation. The U.S. Office of Personnel Management describes integrity testing as an assessment approach relevant to predicting counterproductive work behaviors: OPM—Other Assessment Methods. Sound use also requires evidence of validity, reliability, and fairness, consistent with the Standards for Educational and Psychological Testing.

QUESTION NO: 3

Most theft is committed by:

A. Professionals

B. Organized crime

C. Amateurs

D. Maladjusted criminals

E. Semiprofessionals

ANSWER: C

Explanation:

Amateurs is correct. In protection practice, the greatest volume of theft incidents is typically attributable to opportunistic, nonprofessional offenders rather than to highly skilled or specialized thieves. These individuals commonly exploit an accessible target, weak supervision, inadequate access control, poor inventory accountability, or an immediate chance to take property with a perceived low risk of detection. Their acts may be impulsive or situational, but their cumulative frequency produces a substantial share of overall theft losses.

This distinction matters for a protection professional because controls designed to reduce everyday opportunity can prevent a large number of incidents. Visible guardianship, sound key and access-control practices, surveillance, asset marking, inventory controls, clear reporting procedures, and consistent investigation of loss all increase the perceived likelihood of detection. Situational crime-prevention principles similarly emphasize reducing opportunities and increasing the effort and risk associated with offending. Crime data collection also treats larceny-theft as a high-volume property-crime category, reinforcing the need for broad, routine preventive controls rather than a strategy focused solely on sophisticated offenders. See the FBI Crime Data Explorer and the Center for Problem-Oriented Policing's overview of situational crime prevention.

QUESTION NO: 4

Which of the following may be an indication of a planted bomb?

A. Loose electrical fittings

B. Tin foil

C. Fresh plaster or cement

D. All of the above

E. None of the above

ANSWER: D

Explanation:

All of the above is correct because each listed condition can be a potential visual indicator of a suspicious item or of concealment associated with an improvised explosive device. Loose electrical fittings can indicate altered wiring or the placement of electrical components in an area where they would not normally be present. Tin foil may be associated with improvised device construction, including concealment or components, particularly when found in an unusual location or with other suspicious materials. Fresh plaster or cement can suggest that a void, compartment, or object has recently been concealed or that a location has been altered to hide a device.

These signs must always be evaluated in context. Security personnel should focus on items or conditions that are out of place, recently altered, unattended, or inconsistent with the normal environment. A person who identifies a potentially suspicious device should not touch, move, open, or attempt to investigate it. Instead, they should isolate the area, follow the organization's bomb-threat and emergency procedures, and promptly notify law enforcement or emergency services. The

U.S. Cybersecurity and Infrastructure Security Agency provides guidance on recognizing and responding to suspicious items in its bomb threats resources. The FBI also emphasizes reporting suspicious activity through its counterterrorism guidance.

QUESTION NO: 5

If the agent commits a tort:

A. The agent is personally responsible to the injured party.

B. The agent is not liable if the agent was working for the principal at the time

C. The agent is not liable if acting within the scope of employment.

D. The agent is not liable if the agent has a written contract with the employer

E. None of the above

ANSWER: A

Explanation:

The agent is personally responsible to the injured party. Agency status does not eliminate an individual's direct responsibility for the individual's own tortious conduct. A tort is a civil wrong, such as negligence, assault, trespass, defamation, or property damage, for which the injured party may seek a legal remedy. When an agent commits that wrong, the agent has personally engaged in conduct that can give rise to liability to the harmed person.

In an employment or agency setting, the principal or employer may also face liability under respondeat superior when the tort occurs within the scope of employment. That potential vicarious liability supplements, rather than replaces, the tortfeasor's personal liability. For security leaders, this principle reinforces the importance of effective training, supervision, policies, incident reporting, and insurance planning: organizational accountability may arise from employee actions, while the individual who committed the tort remains accountable for the direct harm caused. The exact outcome in a real dispute can depend on jurisdiction and facts, but the foundational agency-law rule is that an agent is liable for the agent's own torts. See Cornell Law School's overview of agency law and its definition of respondeat superior.

QUESTION NO: 6

The main objective of private security is:

A. To apprehend those who steal property from their firms

B. To protect assets and prevent losses

C. To assist police in investigation of crimes

D. To prevent unauthorized persons from entry on firm's property

ANSWER: B

Explanation:

The main objective of private security is **to protect assets and prevent losses**. Private security is fundamentally a risk-management function: it safeguards an organization's people, property, information, operations, and reputation by identifying threats, assessing vulnerabilities, and implementing proportionate protective measures. Its central emphasis is prevention and loss reduction rather than responding only after an incident has occurred. Effective programs use layered controls that may include security officers, access-control systems, surveillance, policies, training, emergency planning, investigations, and business-continuity measures. These measures are selected and managed to reduce the likelihood and impact of theft, violence, fraud, disruption, and other adverse events. ASIS professional guidance describes security management as protecting organizational assets through a systematic and risk-based approach, consistent with the broad asset-protection and loss-prevention purpose stated here. See ASIS International's overview of the Certified Protection Professional credential at https://www.asisonline.org/certification/cpp/ and its security-risk-management guideline resources at https://www.asisonline.org/publications--resources/standards--guidelines/.

QUESTION NO: 7

In which of the following areas are traditional police responsibilities increasingly shared with private security?

A. Federal properties

B. Urban and suburban

C. Large corporations

D. Public parks

ANSWER: B

Explanation:

Urban and suburban is correct because these environments commonly require a blended public-private approach to safety, order maintenance, crime prevention, and incident response. Dense commercial districts, mixed-use developments, transit-adjacent locations, residential communities, shopping areas, entertainment venues, and business improvement districts create security demands that extend beyond the resources available for routine public-police coverage. Private security personnel therefore provide visible patrols, access control, surveillance monitoring, customer assistance, preliminary incident management, and timely reporting or liaison with law enforcement. This does not transfer core governmental police powers to private personnel; rather, it expands the practical sharing of protective responsibilities through coordination, information exchange, and complementary services.

This arrangement is especially established in urban and suburban settings because property owners, local businesses, community associations, and municipalities can organize and fund security programs focused on specific places and recurring risks. Certified protection professionals should understand the need for clear scope-of-authority definitions, escalation procedures, communications protocols, and cooperative relationships with public law enforcement when managing these programs. ASIS identifies security operations and partnerships as important professional-security competencies; see ASIS Certified Protection Professional. Broader U.S. criminal-justice research also documents the substantial role of private security in protecting people and property alongside public policing; see the Bureau of Justice Statistics private security topic page.

QUESTION NO: 8

Which of the following would be an argument against the use of nonlethal weapons by the security officer?

A. They do not pose a substantial risk of death if used properly.

B. They provide an alternative to guns where the situation requires less than lethal force.

C. Use of nonlethal weapons reduces the risk of death to innocent bystanders.

D. It might escalate confrontations with security officers because offenders would feel less threatened.

E. None of the above.

ANSWER: D

Explanation:

It might escalate confrontations with security officers because offenders would feel less threatened. is an argument against relying on nonlethal weapons. A security officer's use-of-force decision must account not only for the intended physical effect of a tool, but also for whether it will gain control of the subject, stop the harmful behavior, and avoid extending or intensifying the encounter. If an offender perceives the weapon as unlikely to cause meaningful consequences, that perception can reduce deterrence and encourage resistance, aggression, or attempts to disarm the officer. The resulting prolonged confrontation can increase danger to the officer, the offender, and nearby persons.

Less-lethal tools are therefore not simply "safe" substitutes for firearms; they require training, clear policy, situational judgment, and an understanding of their limitations. Their effectiveness can vary according to the subject's behavior, distance, environmental conditions, and the particular device employed. The National Institute of Justice notes that less-

lethal technologies must be assessed for effectiveness and safety in operational contexts, while law-enforcement guidance emphasizes that force options must be evaluated in light of the totality of circumstances. See the National Institute of Justice overview of less-lethal technologies and the U.S. Department of Justice guidance on use-of-force principles.

QUESTION NO: 9

Which of the following would not be considered in the "trade secret" category?

A. Salary data

B. Market surveys

C. Personnel matters

D. Customer usage evaluations

E. All of the above

ANSWER: C

Explanation:

Personnel matters is the best answer because personnel information is ordinarily classified and protected as private or confidential employment information, rather than as a trade secret. A trade secret is business or technical information that derives independent economic value from not being generally known or readily ascertainable and that is subject to reasonable efforts to maintain its secrecy. The key purpose of trade-secret protection is preserving a competitive commercial advantage. Personnel matters, such as employee relations issues, disciplinary records, workplace complaints, and similar human-resources information, require strong safeguards because of privacy, legal, and ethical obligations. However, their protection is generally based on confidentiality, privacy, employment law, and records-management requirements—not on their qualifying as competitively valuable trade-secret information. Security professionals should therefore ensure that personnel records are restricted to authorized users, retained and disposed of according to policy, and handled in compliance with applicable privacy obligations. This classification distinction helps determine the appropriate protective controls, access approvals, and incident-response procedures. The U.S. Legal Information Institute summarizes the trade-secret elements, including economic value from secrecy and reasonable secrecy measures, in its definition of trade secret. The Uniform Law Commission also provides the Uniform Trade Secrets Act.

QUESTION NO: 10

Which of the following is not an element in the classic fire triangle?

A. Oxygen

B. Heat

C. CO2

D. Fuel

E. None of the above

ANSWER: C

Explanation:

CO2 is correct because the classic fire triangle identifies the three conditions necessary for combustion: fuel, heat, and an oxidizing agent, normally oxygen in ordinary fires. Fuel provides the combustible material, heat supplies sufficient energy to bring that material to its ignition temperature, and oxygen supports the oxidation reaction that sustains burning. Carbon dioxide is not one of these required elements. Instead, it is commonly used as a fire-extinguishing agent because it can reduce the concentration of oxygen around a fire and, when discharged from a pressurized extinguisher, can also provide some cooling. This distinction is important in protection and fire-safety planning: understanding the fire triangle helps security and facility professionals select controls that prevent ignition or interrupt combustion, such as removing combustible

materials, controlling ignition sources, or limiting oxygen exposure where feasible. The National Fire Protection Association describes fire as requiring fuel, oxygen, and heat, while OSHA similarly identifies these three components as the basis of the fire triangle. See NFPA fire extinguisher guidance and OSHA fire prevention information.

QUESTION NO: 11

The Department of Defense Personnel Security Questionnaire (Industrial) Form is:

A. DD 16

B. DD 48

C. DD 254

D. DD 441

E. DD 482

ANSWER: B

Explanation:

The Department of Defense Personnel Security Questionnaire (Industrial) was DD Form 48. This historical form was used to collect personal-background information needed to support personnel-security screening and clearance determinations for individuals working in the defense-industrial environment. Its purpose was to document identifying information, residences, employment, education, foreign connections, and other information relevant to a government personnel-security investigation. In the industrial-security context, the form supported the government's assessment of whether an individual could be granted access to classified information while employed by a cleared contractor. DD Form 48 is part of the historical set of Department of Defense forms associated with personnel-security processing; modern security vetting processes have since moved to successor questionnaires and electronic systems. The official Department of Defense forms repository provides access to DoD form records and historical form materials at https://www.esd.whs.mil/Directives/forms/. For current industrial-security and personnel-vetting policy context, consult the Defense Counterintelligence and Security Agency's National Industrial Security Program resources at https://www.dcsa.mil/is/nisp/.

QUESTION NO: 12

Which of the following characteristics describes stimulants as a controlled substance?

A. Younger individuals who use stimulants for a euphoric effect often go on to experiment with other drugs of abuse.

B. Users tend to rely on stimulants to feel stronger, more decisive and self-possessed.

C. Stimulants are usually administered by injection or taken orally.

D. Heavy use could result in psychological dependence.

E. Tolerance develops from heavy use.

F. All of the above.

ANSWER: F

Explanation:

All of the above. is correct because the listed statements collectively describe recognized behavioral, administration, and dependence-related characteristics of stimulant misuse. Stimulants activate the central nervous system and may produce euphoria, increased energy, confidence, alertness, and a subjective feeling of enhanced strength or decisiveness. Those effects can reinforce repeated use, including use by young people seeking euphoric effects and potentially engaging in broader substance experimentation.

Controlled stimulants may be taken orally or injected, among other routes depending on the substance and formulation. With repeated heavy use, users can develop tolerance, meaning greater amounts may be sought to obtain the desired effect. Repeated use can also produce psychological dependence, in which craving and reliance on the substance's perceived emotional or performance effects become central to continued use. These are important protection and workplace-safety concerns because stimulant impairment and withdrawal can affect judgment, behavior, reliability, and risk-taking. The U.S. Drug Enforcement Administration identifies stimulants as substances that increase central nervous system activity and notes their potential for misuse and dependence. See the DEA stimulant fact sheet and the National Institute on Drug Abuse overview of prescription stimulants.

QUESTION NO: 13

Defense Department regulations require the identification card of a defense contractor to include a:

A. Distinctive color coding

B. Thumbprint

C. Photograph of the holder

D. Symbol code

E. All of the above

ANSWER: C

Explanation:

Photograph of the holder is correct. For a defense-contractor identification credential to support access control and personnel verification, it must permit security personnel to compare the person presenting the credential with the individual to whom it was issued. A current photograph is the essential visual identifier for that purpose. It helps guards and other authorized personnel make an immediate identity comparison at entry points, restricted areas, and locations where contractor personnel require recurring access.

This requirement supports the broader Department of Defense personnel-security and physical-security objective of ensuring that access credentials are issued to, used by, and presented only by the authorized individual. A photograph also provides a practical control against credential lending, misuse, and attempted impersonation. Contractor security programs operating under the National Industrial Security Program must establish controls for identifying cleared personnel and protecting classified information; identity verification is a fundamental part of those controls. The governing National Industrial Security Program regulation is available at 32 CFR Part 117. DoD physical-security policy likewise emphasizes identification and access-control measures to protect DoD personnel, property, and activities; see DoD Instruction 5200.08.

QUESTION NO: 14

During a security clearance background investigation, verification of naturalization will primarily be done by:

A. Checking State Department records

B. Checking FBI records

C. Checking records of appropriate U.S. district courts

D. Checking records of the Bureau of Vital Statistics

E. All of the above

ANSWER: C

Explanation:

Checking records of appropriate U.S. district courts is correct because naturalization historically was a judicial process, and the court that granted citizenship created the primary naturalization record. A thorough background investigation seeks

documentary confirmation from the authoritative custodian of the naturalization proceeding, including the petition for naturalization, oath of allegiance, certificate-related records, and the court's final order or decree. The appropriate court is determined by the jurisdiction and time period in which the individual was naturalized. Court records therefore provide direct, reliable evidence that naturalization was legally granted, rather than merely indicating related identity, immigration, or law-enforcement information.

This approach reflects the historical U.S. naturalization framework under which federal, state, and local courts could exercise naturalization authority; federal district courts were among the principal courts maintaining these records. The National Archives notes that naturalization records were created by the courts that processed the petitions, and USCIS similarly describes historical naturalization documentation as records generated through this legal process. For current investigations, records may also be held or accessible through successor custodians depending on the date and jurisdiction, but the essential verification principle remains obtaining confirmation from the authoritative naturalization record source. See National Archives: Naturalization Records and USCIS: Naturalization Records.

QUESTION NO: 15

Technical information used for training, maintenance, and inspection of classified military munitions of war would be classified as:

A. Restricted

B. Classified

C. Top secret

D. Confidential

E. Cosmic

ANSWER: D

Explanation:

Confidential is the appropriate classification for this type of technical munitions information. In the national-security classification system, Confidential is used for information whose unauthorized disclosure reasonably could be expected to cause damage to national security. Technical material supporting the training, maintenance, and inspection of classified munitions can reveal protected capabilities, operating characteristics, readiness-related procedures, vulnerabilities, or safeguarding requirements. Even when it does not contain the exceptionally sensitive strategic or operational content associated with higher classification levels, its release can still create a national-security risk and therefore warrants protection at the Confidential level.

This reflects the principle that classification is based on the expected damage from unauthorized disclosure and must be applied by an authorized original classification authority or under approved classification guidance. Executive Order 13526 identifies Confidential as the level for information reasonably expected to cause damage to national security if disclosed without authorization. Department of Defense classification guidance similarly requires protection of controlled technical military information according to the applicable classification determination. See Executive Order 13526 and the DoD Information Security Program manual.

QUESTION NO: 16

The most important written instructions for a security force are known as:

A. policies.

B. procedures

C. post orders.

D. operational orders.

ANSWER: C

Explanation:

post orders. is correct. Post orders are the written directions that govern how security officers perform duties at a specific assignment, post, facility area, or access point. They translate the organization's security policies, risk treatment decisions, and operating procedures into practical, post-specific instructions that an officer can apply during a shift. Effective post orders identify the purpose of the post, required patrol or access-control activities, reporting and escalation requirements, emergency actions, equipment use, communications procedures, and any client- or site-specific restrictions. Because they establish the expected actions and responsibilities for personnel deployed at individual posts, they are a fundamental management and accountability tool for a security force. Supervisors use current post orders for training, post inspections, and performance evaluation, while officers rely on them to provide consistent service and make appropriate notifications when conditions depart from normal operations. ASIS guidance on security management emphasizes documented operational direction, clear assignment responsibilities, and training aligned to the duties personnel are expected to carry out. See ASIS International's Certified Protection Professional (CPP) certification overview and its security standards and guidelines resources.

QUESTION NO: 17

The Privacy Act of 1974 provides which of the following safeguards?

A. Permits individuals to gain access to certain information pertaining to themselves in federal agency records

B. Permits individuals to determine what records pertaining to themselves are collected and maintained by federal agencies

C. Permits individuals to prevent certain records pertaining to themselves from being used or made available for another purpose without their consent

D. Requires federal agencies to be subject to civil suits for any damages that may occur as a result of willful or intentional action that violates an individual's rights under the Privacy Act of 1974

E. All of the above

ANSWER: E

Explanation:

All of the above is correct because the Privacy Act of 1974 establishes a set of interrelated safeguards governing records about individuals that are maintained by U.S. federal agencies in systems of records. It gives an individual a right to learn whether an agency maintains records about them and, subject to statutory exemptions, to request access to those records. The Act also requires agencies to publish notices describing their systems of records, including the categories of individuals and records covered, so that collection and maintenance practices are visible to the public.

Its disclosure controls are equally important: an agency generally may not disclose a record contained in a system of records without the written consent of the person to whom it pertains, unless a specified statutory exception applies. This supports purpose limitation by restricting reuse or release of personal information beyond the conditions authorized by law. Finally, the Act provides civil remedies in defined circumstances when an agency intentionally or willfully fails to comply with its requirements in a manner that adversely affects an individual, including provisions for damages and litigation costs where applicable. These protections are summarized by the U.S. Department of Justice in its Privacy Act of 1974 overview and codified at 5 U.S.C. § 552a.

QUESTION NO: 18

Any formula, pattern, device, or compilation of information that is used in one's business and that gives you an opportunity to gain an advantage over competitors who do not use it or know about it is:

A. A patent

B. A trade secret

C. A monopoly

D. Copyrighted material

E. None of the above

ANSWER: B

Explanation:

A trade secret is correct because the description tracks the established definition of a trade secret: commercially valuable information, such as a formula, pattern, device, method, technique, process, or compilation, that derives independent economic value from not being generally known or readily ascertainable by others who could gain economic value from its use or disclosure. Its value is tied directly to the competitive advantage created by its confidentiality.

For protection professionals, trade-secret protection has important operational implications. The organization must take reasonable measures to preserve secrecy, which can include information-classification policies, need-to-know access controls, confidentiality and nondisclosure agreements, secure handling procedures, monitoring, and incident-response processes for suspected unauthorized disclosure. Unlike some intellectual-property rights, trade-secret protection can continue as long as the information remains secret and retains economic value because of that secrecy. The legal framework in the United States is reflected in the Uniform Trade Secrets Act and the federal Defend Trade Secrets Act. The Legal Information Institute summarizes the definition and protections at Cornell Law School's Trade Secret overview. The U.S. Patent and Trademark Office also describes how trade secrets protect confidential business information at USPTO Trade Secret Policy.

QUESTION NO: 19

Responsibility for shutdown supervision should be assigned by the disaster plan to a facility's engineering service The actual shutdown should be accomplished by:

A. a maintenance worker.

B. senior management.

C. the plant manager

D. employees familiar with the process.

ANSWER: D

Explanation:

The correct answer is **"employees familiar with the process."** A disaster plan should distinguish between supervisory authority and task execution. Engineering services may be assigned responsibility for coordinating and supervising a shutdown because they understand facility systems, dependencies, and the overall safe sequence of actions. However, the physical shutdown of machinery, utilities, processes, or specialized equipment must be performed by personnel who are trained and authorized to operate those particular systems. These employees know the normal operating procedures, emergency shutdown steps, isolation points, hazards, and safeguards associated with their work. Assigning the action to process-familiar personnel helps ensure the shutdown is completed promptly, in the correct order, and without creating additional danger to people, property, or operations. Effective emergency and disaster planning therefore identifies both the person or function accountable for command and the qualified individuals responsible for carrying out critical procedures. This approach aligns with OSHA emergency-action-plan guidance, which calls for clear procedures and assigned responsibilities, as well as FEMA continuity planning principles requiring defined roles and trained personnel for essential functions. See OSHA Emergency Action Plans and FEMA Continuity Guidance.

QUESTION NO: 20

"Strict liability in tort" is also known as:

A. Gross negligence

B. Comparative negligence

C. Intentional liability

D. Last clear chance

E. Liability without fault

ANSWER: E

Explanation:

Strict liability in tort is also known as **liability without fault**. Under this doctrine, a party may be legally responsible for harm caused by a particular activity or product even when the injured person does not need to prove that the responsible party acted negligently or intended to cause harm. The focus is on the nature of the activity, the product defect, and the causal connection to the injury rather than on whether reasonable care was exercised.

In security and risk-management contexts, this principle is important when evaluating organizational exposure arising from inherently dangerous activities, hazardous materials, dangerous animals, or certain product-related harms. A protection professional should recognize that ordinary safeguards and careful conduct may not always eliminate civil-liability exposure where strict-liability rules apply. Risk treatment may therefore require avoidance, contractual risk transfer where legally permissible, insurance, specialized controls, and informed legal counsel. The Legal Information Institute describes strict liability as liability imposed without a finding of fault, particularly in areas such as abnormally dangerous activities and product liability. See Cornell Law School's Legal Information Institute: Strict Liability and Cornell Law School's Legal Information Institute: Tort.

QUESTION NO: 21

An ADP system that operates in a manner in which at least some of the users with access to the system have neither a security clearance nor a need-to-know status for all classified information that is in the system, but in a manner that the cognizant security officer or a higher authority has determined that the necessary degree of security has been achieved and maintained, is known as:

A. Limited Security Mode

B. Classified Security Mode

C. Controlled Security Mode

D. Restricted Security Mode

E. Dedicated Security Mode

ANSWER: C

Explanation:

Controlled Security Mode is correct because it describes a legacy classified automated data-processing operating mode in which all users are not necessarily cleared for, or authorized by need-to-know for, all classified information resident in the system. The defining safeguard is not universal user eligibility; rather, it is the determination by the cognizant security authority that the system's combination of technical, procedural, personnel, and physical controls provides and maintains the required degree of protection. Such a determination is an accreditation decision: the responsible authority accepts that the implemented protections adequately manage the risks of access by users who do not hold clearance or need-to-know for every item of classified data that the system processes or stores.

The wording in the question closely follows the historical government terminology used for classified-system security modes. These concepts developed in the era of trusted computer-system evaluation and remain useful for understanding how security authorization, access restrictions, and compensating controls support protection of classified information. The U.S. Department of Defense Trusted Computer System Evaluation Criteria provides foundational context for trusted-system security concepts at NIST CSRC: DoD 5200.28-STD. Current U.S. requirements for safeguarding classified information in contractor environments are available in the National Industrial Security Program Operating Manual regulations.

QUESTION NO: 22

While conducting an interview, the most important initial objective for the investigator to accomplish is to:

A. obtain an understanding of all the facts of the case.

B. establish a favorable rapport with the interviewee.

C. use all applicable means to get the interviewee to release information.

D. prepare copious notes of all events detailed by the interviewee.

ANSWER: B

Explanation:

Establish a favorable rapport with the interviewee is the most important initial objective because effective investigative interviewing depends on voluntary, accurate, and complete communication. At the start of an interview, the investigator should create an environment in which the interviewee feels respected, understands the purpose and process of the discussion, and is willing to speak candidly. A professional introduction, appropriate demeanor, active listening, and nonjudgmental questions help reduce anxiety and support cooperation. This foundation enables the investigator to assess the interviewee's account, clarify relevant details, and obtain reliable information as the interview progresses. Rapport does not mean agreeing with the interviewee or compromising objectivity; it means establishing sufficient trust and communication to conduct the interview fairly and productively. The approach is consistent with evidence-based interviewing principles that emphasize rapport, respectful treatment, and information gathering rather than confrontational tactics. The U.S. Office of Justice Programs describes rapport as a key component of effective investigative interviewing, while the College of Policing's investigative-interviewing guidance emphasizes planning and communication practices that promote accurate accounts. See NIJ: Investigative Interviewing and College of Policing: Investigative Interviewing.

QUESTION NO: 23

In the management of an incident, which group has the capability to make informed decisions using available information?

A. Bomb evaluation and assessment response (BEAR) team

B. Bomb assessment team (BAT)

C. Bomb threat response team (BTRT)

D. Threat evaluation team (TET)

ANSWER: D

Explanation:

Threat evaluation team (TET) is correct because incident management requires a designated, multidisciplinary group that can rapidly collect, assess, validate, and synthesize the information available at the time of an event. A TET applies relevant security, operational, legal, human-resources, safety, and emergency-management expertise to determine the nature, credibility, urgency, and likely consequences of a threat. It then provides decision-makers with a defensible assessment and recommends proportionate protective actions, such as notification, escalation, protective measures, continuity actions, or coordination with public authorities. This structure supports informed decision-making even when information is incomplete, evolving, or contradictory—a normal condition in security incidents. The team's value lies in combining available intelligence with organizational knowledge, defined response procedures, and risk-based judgment rather than relying on one individual's perspective. ASIS guidance emphasizes structured threat assessment and multidisciplinary intervention processes as components of effective workplace violence and threat-management programs. The U.S. Cybersecurity and Infrastructure Security Agency likewise describes assessment teams as a means to evaluate reported threat information and support an appropriate response. See ASIS Standards and Guidelines and CISA Bomb Threat Guide.

QUESTION NO: 24

Depressants of various types are included in Schedules II, III, and IV of the Controlled Substances Act. Which of the following does not apply to the use of depressants?

A. Depressants have a high potential for abuse.

B. Some drug abusers often resort to the use of depressants to soothe their nerves after the use of stimulants.

C. The use of depressants compounded with alcohol can cause death.

D. Moderate depressant poisoning closely resembles intoxication from alcohol.

E. One of the recognized features from the use of depressants is that tolerance will not develop.

ANSWER: E

Explanation:

“One of the recognized features from the use of depressants is that tolerance will not develop.” is the statement that does not apply. Tolerance can develop with repeated use of central nervous system depressants, meaning that a person may require progressively larger doses to obtain the initially experienced effect. This is a clinically significant feature of repeated depressant use and is closely related to the risks of physical dependence and withdrawal. Depressants include drug classes such as sedative-hypnotics, barbiturates, and benzodiazepines; although individual substances have differing medical indications and control schedules, repeated nonmedical or prolonged use can lead to tolerance. The Drug Enforcement Administration specifically identifies tolerance and dependence as risks associated with depressant misuse. Increasing doses in response to tolerance can substantially increase the risk of dangerous respiratory depression, particularly when other central nervous system depressants are also present. Thus, the claim that tolerance will not develop contradicts established pharmacological and drug-control guidance. See the DEA’s overview of depressants and the National Institute on Drug Abuse discussion of prescription CNS depressants.

QUESTION NO: 25

The removal of any suspected bomb should be by:

A. A proprietary guard force

B. Office employees

C. Professional bomb-disposal personnel

D. The patrol office of the police department

E. None of the above

ANSWER: C

Explanation:

Professional bomb-disposal personnel is correct because a suspected explosive device must be handled only by trained, equipped, and authorized bomb technicians. Their specialized training includes assessing explosive hazards, establishing safety measures and exclusion zones, using appropriate protective equipment and remote tools, and selecting safe render-safe, removal, or disposal procedures. Security personnel and facility employees have an essential supporting role: promptly report the suspicious item, avoid touching or moving it, isolate the area, initiate emergency procedures, and support responding public-safety agencies. They should not attempt to inspect, transport, or remove a suspected device. A sound protective-security emergency plan identifies in advance how law enforcement and explosive-ordnance-disposal resources will be contacted and integrated into the incident response. The U.S. Cybersecurity and Infrastructure Security Agency advises personnel to avoid touching suspicious items and to notify authorities, while the FBI emphasizes reporting suspicious packages or devices to law enforcement. These practices protect life safety, preserve the scene for professional assessment, and reduce the risk that an improvised explosive device could be initiated during handling. See CISA Bombing Prevention and FBI Counterterrorism.

QUESTION NO: 26

A controlled area established to safeguard classified material that, because of its size or nature, cannot be adequately protected by other prescribed safeguards is termed to be:

A. A restricted area

B. A classified area

C. A closed area

D. A limited area

E. None of the above

ANSWER: C

Explanation:

A closed area is the correct term. In U.S. government and defense security terminology, a closed area is specifically established to protect classified information or material that cannot be feasibly secured through normal methods because of its size, quantity, physical characteristics, operational use, or nature. Examples can include large classified equipment, extensive technical displays, maps, workstations, or materials that must remain in place to support an ongoing mission.

The designation permits the organization to apply layered physical-security and access-control measures to the entire defined space rather than relying solely on containers, safes, or individually securing each item. Such measures commonly include clearly defined boundaries, access limited to authorized personnel, visitor controls, end-of-day security procedures, and protective measures appropriate to the classification level and threat environment. The objective is to ensure that classified material remains protected from unauthorized access, observation, removal, or compromise even when conventional storage safeguards are impractical.

This usage is reflected in Department of Defense guidance addressing the protection of classified information and the establishment of closed areas. See the DoD Manual 5200.01, Volume 3 and the National Industrial Security Program Operating Manual.

QUESTION NO: 27

The principal purpose of a business impact analysis is to determine:

A. The operational and financial effects of disruption to critical activities

B. The identities and motives of all potential adversaries

C. The number of security officers required for routine patrols

D. The replacement cost of every physical asset

E. The legal authority of emergency responders

ANSWER: A

Explanation:

The principal purpose of a business impact analysis is to determine the operational and financial effects of disruption to critical activities over time. The analysis identifies essential products and services, dependencies, maximum tolerable downtime, recovery priorities, and the resources needed to resume operations. These findings provide the basis for business continuity and disaster recovery strategies.

A business impact analysis is distinct from a threat assessment. A threat assessment considers events or adversaries that could cause harm, whereas the business impact analysis concentrates on the consequences to the organization if a process, system, facility, supplier, or service becomes unavailable. The analysis should involve process owners and be reviewed as business operations change. See Ready.gov business emergency planning guidance and ISO 22301 Business Continuity Management Systems.

QUESTION NO: 28

When homicide is committed by accident and misfortune in doing any lawful act by lawful means with usual ordinary caution, it is' known as:

A. General homicide

B. Justifiable homicide

C. Excusable homicide

D. Voluntary manslaughter

E. Involuntary manslaughter

ANSWER: C

Explanation:

Excusable homicide is the correct classification because the facts describe a death occurring accidentally while a person is engaged in a lawful act, uses lawful means, and exercises ordinary caution, with no unlawful intent. In the traditional common-law terminology reflected in many criminal statutes, this type of accidental killing is excused because the actor's conduct is neither criminally intended nor negligent. The key elements are accident or misfortune, a lawful underlying activity, lawful conduct, and the use of ordinary care. Together, those elements distinguish an excused accidental death from an unlawful killing.

For example, California's statutory formulation expressly identifies homicide as excusable when it occurs "by accident and misfortune" during a lawful act performed with "usual and ordinary caution" and without unlawful intent. This wording closely tracks the language in the question and supports the classification. See California Penal Code section 195. Legal terminology and precise statutory definitions can vary by jurisdiction, but the stated rule is a classic description of excusable homicide. For general legal background on homicide classifications, see Cornell Law School's Legal Information Institute.

QUESTION NO: 29

The control of traffic through entrances and exits of a protected area is referred to as:

A. Access control

B. Patrol management

C. Traffic stops

D. Traffic management

E. None of the above

ANSWER: A

Explanation:

Access control is the correct term for controlling the movement of people, vehicles, and, where applicable, materials through the entrances and exits of a protected area. In protection practice, access control is a preventive security function that determines who or what is authorized to enter, leave, or move within a defined space. It may involve guards, visitor-management procedures, credentials, keys, locks, turnstiles, vehicle barriers, electronic access-control systems, and screening procedures. Effective access control applies authorization rules consistently, verifies identity or credentials as appropriate, records activity when needed, and supports the protection of personnel, assets, information, and operations. The reference to a "protected area" and to entrance and exit traffic specifically describes this core security function rather than general traffic-flow or patrol activities. ASIS guidance recognizes access control as a foundational element of physical security, and it is commonly integrated with perimeter protection, surveillance, alarm monitoring, and incident-response processes. See ASIS International's access-control resources and the U.S. Cybersecurity and Infrastructure Security Agency's physical-security guidance.

QUESTION NO: 30

After implementing a new access-control system, the security manager should use periodic testing primarily to:

A. Verify that the system and related procedures continue to operate as intended

B. Eliminate the need for preventive maintenance

C. Demonstrate that no unauthorized access can ever occur

D. Replace all incident investigations

E. Determine which employees should receive promotions

ANSWER: A

Explanation:

Verify that the system and related procedures continue to operate as intended is correct because security controls can degrade over time through equipment failure, configuration changes, credential errors, procedural drift, maintenance deficiencies, or changing operational conditions. Periodic testing identifies whether access is appropriately granted, denied, logged, monitored, and reviewed in accordance with the control objectives.

Testing should be planned, authorized, documented, and conducted in a manner that does not create unnecessary operational or life-safety risk. Results should be analyzed to identify root causes, corrective actions, responsible parties, and follow-up validation. Installation acceptance testing alone is insufficient because it confirms initial operation but does not establish continuing effectiveness. See the CISA physical security resources and NIST Cybersecurity Framework.

QUESTION NO: 31

If a private security officer violates the restriction of the laws of arrest that apply to him or her, he or she may:

A. Jeopardize the case against the subject

B. Be subject to criminal charges

C. Be held liable for damages in a civil suit

D. All of the above

E. None of the above

ANSWER: D

Explanation:

All of the above is correct because a private security officer who exceeds the legal authority applicable to a private-person arrest can create consequences in several legal areas at once. An unlawful detention or arrest may undermine the subsequent prosecution, particularly where the officer's actions affect the reliability, admissibility, or handling of evidence and witness information. The officer also may face criminal exposure when the conduct satisfies the elements of an offense, such as unlawful restraint, assault, or other jurisdiction-specific offenses. In addition, the detained person may bring a civil claim for harms arising from an improper arrest or detention, including claims commonly described as false imprisonment or false arrest; the employer may also face liability depending on the facts, employment relationship, and applicable law. Security professionals must therefore understand the limited arrest powers granted to private persons in their jurisdiction, use only reasonable force when authorized, promptly involve law enforcement, and document the circumstances and basis for the detention. The Legal Information Institute describes false imprisonment as the unlawful confinement of a person without consent or legal authority: Cornell Law—False Imprisonment. The U.S. Department of Justice also provides an overview of civil rights enforcement involving law-enforcement misconduct: DOJ—Law Enforcement Misconduct.

QUESTION NO: 32

Which of the following is not true regarding electronic eavesdropping?

A. An effective countermeasure to detect evidence of electronic eavesdropping in telephone equipment should be conducted by a person who is technically familiar with such equipment.

B. An effective countermeasure would be to conduct a physical search as well as an electronic search.

C. All wiring should be traced and accounted for.

D. A listening device installed in a wire will cause a crackling sound, click, or other noise that can be heard on the line.

E. None of the above.

ANSWER: D

Explanation:

“A listening device installed in a wire will cause a crackling sound, click, or other noise that can be heard on the line.” is the statement that is not true. Audible anomalies are not a dependable indicator of an interception device. Electronic eavesdropping equipment can be designed, installed, or configured to operate without producing perceptible line noise; a passive connection in particular may create no obvious audible symptom. Conversely, ordinary telephone-line conditions, switching activity, poor connections, and electrical interference can produce clicks or crackling without indicating surveillance. Security personnel therefore should not treat listening tests as a reliable detection method or infer that a quiet line is free from compromise.

A competent technical-surveillance countermeasure process relies on appropriately qualified personnel and a structured inspection of the environment, including physical examination of equipment and cable paths, verification of expected wiring, and suitable technical testing. This risk-based approach is consistent with NIST guidance that calls for assessing threats and vulnerabilities and selecting security controls based on the resulting risk determination. See NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments and the NIST Cybersecurity Framework for the broader principle of identifying and managing security risks using evidence-based safeguards.

QUESTION NO: 33

The class of person under a duty to safeguard a proprietary secret is known as a(n):

A. Agent

B. Proprietary security employee

C. Fiduciary

D. Business associate

E. None of the above

ANSWER: C

Explanation:

Fiduciary is correct because a fiduciary relationship imposes heightened duties of loyalty, trust, and care on a person entrusted with another party’s interests or confidential property. In a protection and proprietary-information context, this duty includes safeguarding confidential business information or trade secrets when the information has been entrusted to the person through such a relationship. The duty may arise from the nature of the relationship, from an express confidentiality commitment, or both.

Trade-secret law recognizes that misappropriation can occur when a person discloses or uses a trade secret without consent while under a duty to maintain its secrecy or limit its use. This principle is reflected in the Uniform Trade Secrets Act’s definition of misappropriation, which addresses information acquired under circumstances giving rise to such a duty. A fiduciary is therefore an appropriate term for the class of trusted persons who must protect proprietary secrets. Security professionals should identify fiduciary and other confidential relationships, define information-handling requirements, and implement controls that preserve secrecy throughout access, use, storage, and separation from the organization. See the Uniform Trade Secrets Act and Cornell Law School’s fiduciary duty overview.

QUESTION NO: 34

Which of the following is not recommended as a preventive measure to prevent panic?

A. Give people a routine to keep down anxieties.

B. Don't emphasize discipline.

C. Provide full and appropriate information to combat ignorance.

D. Control rumors.

E. None of the above.

ANSWER: B

Explanation:

“Don't emphasize discipline.” is the measure that is not recommended. Effective panic prevention depends on creating an orderly, predictable environment in which people understand what is expected of them and can follow clear directions. Appropriate discipline does not mean using unnecessarily harsh or confrontational control; rather, it means establishing and communicating orderly procedures, maintaining supervision, and encouraging compliance with safety instructions. These measures help reduce uncertainty and disorganized behavior, both of which can escalate fear in an emergency.

For security professionals, disciplined organization supports calm decision-making and coordinated movement. Personnel should communicate instructions confidently and consistently, use established emergency procedures, and manage the environment so occupants perceive that the situation is being handled competently. This approach aligns with recognized emergency-management guidance emphasizing clear leadership, coordinated incident management, and effective communication during incidents. The U.S. Federal Emergency Management Agency describes the Incident Command System as a standardized approach for command, control, and coordination at incidents: FEMA National Incident Management System. Guidance on crisis and emergency risk communication likewise emphasizes timely, credible information and action-oriented messages that help people respond appropriately: CDC Crisis and Emergency Risk Communication.

QUESTION NO: 35

Which of the following is considered to be the most resistant to a blast explosion?

A. Steel-frame building walls

B. Thick brick or concrete walls

C. Thick earthen barricades

D. Thick reinforced concrete walls

E. Wire-reinforced glass windows

ANSWER: D

Explanation:

Thick reinforced concrete walls are the most blast-resistant choice because reinforced concrete combines the high compressive strength and mass of concrete with the tensile strength, ductility, and continuity provided by embedded reinforcing steel. Blast loading produces an exceptionally rapid, high-pressure impulse followed by dynamic structural response. A thick reinforced-concrete wall can distribute that loading through the wall and its reinforcement, resist flexure and shear, and remain comparatively intact even when it sustains cracking or localized spalling. This capacity to deform while retaining structural continuity is central to blast-resistant design.

Effective blast performance depends on more than material alone: wall thickness, reinforcement detailing, anchorage to the structural frame, opening protection, stand-off distance, and the magnitude and location of the explosive charge all affect the outcome. Nonetheless, for a fixed wall-type comparison, thick reinforced concrete is a well-established protective

construction material. FEMA's guidance on reducing building vulnerability identifies reinforced concrete construction and properly detailed structural systems as key elements in resisting explosive blast effects. The Whole Building Design Guide likewise emphasizes ductile, continuous, reinforced structural components in blast-resistant design. See FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings and the Whole Building Design Guide: Designing Buildings to Resist Blast Effects.

QUESTION NO: 36

The National Bomb Data Center is operated by the:

A. CIA

B. FBI

C. ATF

D. LEAA

E. Census Bureau

ANSWER: B

Explanation:

The correct answer is **FBI**. The National Bomb Data Center (NBDC) is a component of the Federal Bureau of Investigation's Laboratory Division. It serves as the United States' central repository and information-sharing resource for bombing incidents, explosive devices, and related threats. Its mission supports public-safety bomb squads, law-enforcement agencies, military partners, and other stakeholders by collecting, analyzing, and disseminating information on explosive incidents and trends.

For protection professionals, this role is important because NBDC products and resources can inform organizational bomb-threat planning, incident reporting, threat assessment, and liaison with law enforcement after an explosive-related event. The center also supports national efforts to identify patterns in explosive-device use and to improve prevention, preparedness, response, and investigative capabilities. The FBI identifies the NBDC among its operational resources for explosive-related intelligence and technical support, confirming that it is FBI-operated. See the FBI's Explosives program information and its Laboratory Services overview.

QUESTION NO: 37

Which of the following distinguishes embezzlement from other kinds of theft of corporate property or funds?

A. Embezzlement can be detected only through an audit or accounting discrepancy.

B. In embezzlement, the employee breaches a trust by stealing assets entrusted to him/her.

C. Embezzlement is a "white collar" crime most often perpetrated by senior managers.

D. It is not necessary to prove criminal intent in an embezzlement case.

ANSWER: B

Explanation:

"In embezzlement, the employee breaches a trust by stealing assets entrusted to him/her." is correct because the defining feature of embezzlement is the fraudulent conversion or appropriation of property by a person who initially possessed or controlled it lawfully due to a position of trust. In a corporate environment, this commonly involves an employee, manager, agent, or other custodian who has authorized access to company money, inventory, records, or other assets and intentionally uses those assets for an unauthorized personal purpose. The property is therefore not simply taken by an outsider or obtained through an initial unlawful taking; it was entrusted to the individual before the dishonest conversion occurred. This breach-of-trust element is central to security investigations of internal theft and fraud because investigators must establish the entrusted relationship, the person's authorized custody or control, the conversion of the asset, and

evidence supporting intentional misconduct. The precise statutory elements and terminology can vary by jurisdiction, but the core concept consistently distinguishes embezzlement from other theft offenses. The Legal Information Institute's definition of embezzlement describes it as the fraudulent conversion of property by someone in lawful possession of it. The U.S. Department of Justice's Criminal Resource Manual likewise addresses embezzlement as misuse of property entrusted to the offender.

QUESTION NO: 38

A system whereby the alarm signal is heard only in the immediate vicinity of the protected area is known as a:

A. Local alarm system

B. Proprietary system

C. Central alarm system

D. Portable alarm system

E. None of the above

ANSWER: A

Explanation:

Local alarm system is correct because it provides audible or visible notification at, or immediately adjacent to, the protected premises. Its essential characteristic is that the alarm annunciation is confined to the local area so that people nearby can hear the signal and take an appropriate response, such as investigating the condition, evacuating, or contacting emergency services. The signal is not dependent on being received and acted on by an off-site monitoring facility or remote supervising location.

This terminology is consistent with the regulatory distinction between local alarm systems and systems that transmit alarm information elsewhere. OSHA defines a local fire alarm system as an alarm system that sounds an audible signal at the protected premises and does not transmit a signal to a municipal fire department or other remote location. Although the question uses general alarm-system terminology rather than specifically fire alarms, the defining principle is the same: notification is limited to the immediate protected location. See 29 CFR § 1910.163, Fire detection systems. For broader alarm and signaling-system terminology and application, consult the National Fire Protection Association's NFPA 72, National Fire Alarm and Signaling Code.

QUESTION NO: 39

The federal trafficking penalty for a Schedule I narcotic that is the first offense is:

A. 5 years in prison and/or a $10,000 fine

B. 10 years in prison and/or a $20,000 fine

C. 15 years in prison and/or a $25,000 fine

D. 20 years in prison and/or a $30,000 fine

E. 30 years in prison and/or a $50,000 fine

F. Up to 20 years in prison and/or a fine of up to $1,000,000

ANSWER: F

Explanation:

For an unspecified first federal trafficking offense involving a Schedule I controlled substance, the applicable general federal penalty is imprisonment for up to 20 years and a fine of up to $1,000,000 for an individual. This reflects 21 U.S.C. § 841(b)(1)(C), the default penalty provision for distribution, manufacture, or possession with intent to distribute a Schedule I or

II controlled substance when the question does not identify a drug quantity that triggers a separate mandatory-minimum sentencing tier. The statute also permits both imprisonment and a fine, so “and/or” appropriately communicates that a court may impose either sanction or both, within statutory and sentencing-guideline limits. Actual sentencing depends on factors such as the substance and quantity involved, aggravating conduct, criminal history, and whether serious bodily injury or death resulted. Larger specified quantities can trigger materially different mandatory minimums and maximum penalties. The current statutory text is available at 21 U.S.C. § 841. The U.S. Sentencing Commission also provides federal drug-offense sentencing resources at USSC Chapter 2, Part D.

QUESTION NO: 40

Insurance is a form of risk:

A. spreading.

B. avoidance.

C. transfer.

D. reduction

ANSWER: C

Explanation:

Insurance is a form of risk **transfer**. In return for a premium, an organization contractually transfers all or part of the financial consequences of specified accidental losses to an insurer. The organization still owns and must manage the underlying exposure: a fire, liability claim, natural hazard, or interruption may still occur. However, subject to the policy’s terms, limits, deductibles, exclusions, and conditions, the insurer assumes responsibility for indemnifying covered loss. This makes insurance particularly useful for risks that cannot be eliminated or economically controlled to an acceptable level, but whose potential financial impact could exceed the organization’s ability or willingness to absorb it.

In security risk management, insurance should be selected after the organization identifies and assesses its exposures, implements reasonable loss-prevention and loss-control measures, and determines its risk appetite. It supports organizational resilience by helping provide funds for recovery following a covered event; it is not itself a physical security control. The contractual allocation of the financial burden is the essential feature that makes insurance risk transfer. The Insurance Information Institute describes insurance as a mechanism for transferring risk from an individual or business to an insurance company: Insurance Information Institute: What Is Insurance?. ISO 31000 also recognizes risk treatment as involving options that can include sharing risk: ISO 31000:2018 Risk Management.

QUESTION NO: 41

Which of the following is not usually applicable to a confession?

A. It was voluntary.

B. It was made subsequent to commission of a wrongful act.

C. It is often applied to civil transactions.

D. It gives no inference other than guilt.

E. It is an admission of guilt.

ANSWER: C

Explanation:

It is often applied to civil transactions. is correct because a confession is a criminal-law evidentiary concept: a person’s voluntary statement acknowledging guilt for an offense. Its defining subject is criminal culpability, rather than responsibility or statements arising in ordinary civil dealings. Civil disputes may involve admissions by a party, such as statements relevant to a contract, debt, injury, or other claimed liability, but those statements are not ordinarily characterized as confessions. The

distinction matters in investigations and case preparation because investigators should accurately identify whether a subject has made a full acknowledgment of criminal guilt or has merely made an admission concerning a fact or circumstance. A confession generally has particular evidentiary and constitutional considerations, including voluntariness and the circumstances under which it was obtained. Cornell Law School's Legal Information Institute describes a confession as an admission of guilt for a crime and addresses its role in criminal procedure: Cornell Law School, "Confession". The treatment of party admissions as evidence is separately reflected in the Federal Rules of Evidence, which include opposing-party statements among exclusions from hearsay: Federal Rule of Evidence 801.

QUESTION NO: 42

Most deaths from fire are caused by:

A. Visible fire

B. Panic

C. Smoke or heat

D. Inexperienced firefighters

E. Inadequate equipment

ANSWER: C

Explanation:

Smoke or heat is correct because the principal life-threatening hazards in most structural fires are smoke inhalation and exposure to hot, toxic fire gases, often before flames directly reach occupants. Combustion produces a rapidly changing mixture that can include carbon monoxide, hydrogen cyanide, irritant gases, and oxygen-depleted air. Inhaling these products can impair judgment, cause disorientation or incapacitation, and quickly lead to unconsciousness, preventing a person from escaping. Heated smoke can also injure the respiratory tract and lungs. The U.S. Fire Administration emphasizes that smoke is poisonous and that people should get out immediately when a smoke alarm sounds, rather than attempting to locate the fire or retrieve belongings. This supports the protection-management priority of early detection, alarm notification, prompt evacuation, and maintaining tenable egress conditions. Fire-safety education should reinforce crawling low beneath smoke only as needed to reach an exit, using planned escape routes, and remaining outside after evacuation. See the U.S. Fire Administration's home fire escape planning guidance and the National Fire Protection Association's home fire safety resources.

QUESTION NO: 43

Estimates as to the number of security officers - both contract and proprietary - in the United States is approximately:

A. 250,000

B. 300,000

C. 500,000

D. 700,000

E. 1,000,000+

ANSWER: E

Explanation:

1,000,000+ is the best answer. The U.S. private-security workforce is very large, encompassing officers employed directly by organizations (proprietary security) and personnel supplied by contract guard companies. In the context of protection-management education and industry estimates, the combined population has long been described as exceeding one million officers. This scale reflects the broad use of security personnel across commercial properties, healthcare, education, critical infrastructure, residential communities, retail, events, transportation, and government-support environments.

Current federal occupational data also supports using a figure above one million as the appropriate approximation. The U.S. Bureau of Labor Statistics' Occupational Employment and Wage Statistics identifies security guards as a major occupation with employment measured in the millions when considering the nationwide protective-services labor market and the occupation's broad deployment. Although occupational datasets and industry estimates can differ in their definitions, coverage dates, and treatment of related roles, they consistently support the conclusion that the total number of contract and proprietary security officers is well beyond the smaller figures listed. See the BLS Security Guards occupational employment data and ASIS's security management professional resources.

QUESTION NO: 44

The final step in conducting a security risk analysis is consideration of the cost versus the benefit of:

A. human resources strategy.

B. security strategy.

C. insurance.

D. risk strategy.

ANSWER: B

Explanation:

Security strategy. Once assets, threats, vulnerabilities, likelihood, and consequence have been assessed, the organization must decide how it will treat the risks identified. A security strategy translates that analysis into a coordinated set of safeguards, procedures, technologies, personnel measures, and management actions. Comparing implementation and ongoing operating costs against the expected benefit—such as reduced likelihood or impact of loss, improved resilience, protection of people and assets, and support for business objectives—helps ensure that selected controls are proportionate to the risk and economically justifiable. This is a core risk-treatment decision: the organization should invest in measures that reduce risk to an acceptable level while using resources responsibly. The assessment therefore culminates not merely in identifying exposures, but in selecting and prioritizing a viable security strategy based on its anticipated risk-reduction value. NIST's risk-management guidance describes the use of risk assessment results to inform response and control decisions, while its security-control guidance emphasizes tailoring safeguards to organizational risk and mission needs. See NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments and NIST SP 800-53 Rev. 5, Security and Privacy Controls.

QUESTION NO: 45

Which of the following is considered to be an approved method of protecting vital records?

A. On-site storage in vaults or safes

B. Protection of original vital records

C. Natural dispersal within an outside organization

D. Planned dispersal of copies of vital records

E. All of the above

ANSWER: E

Explanation:

All of the above is correct because a sound vital-records protection program uses complementary controls to ensure that records essential to continuity, legal rights, financial accountability, and recovery remain available after an incident. Physical protection of originals in appropriately rated vaults or safes reduces exposure to fire, theft, water damage, and unauthorized access. Identifying and protecting the original vital record also ensures that the authoritative source is preserved with suitable handling, access, and retention controls. Dispersal provides resilience when a single facility or records repository becomes unavailable: records may be naturally dispersed through normal distribution to organizational locations, while

planned dispersal deliberately places duplicate copies at separate, suitably protected sites. In practice, the selection of a method should follow the organization's business-impact analysis, record criticality, recovery-time needs, media format, and threat environment. The goal is not merely to store records securely, but to ensure that usable and current information can be retrieved when normal operations are disrupted. The U.S. National Archives describes vital records as those needed to resume operations and protect rights and interests, and emphasizes planning for their protection and availability. See National Archives vital records guidance and 36 CFR Part 1236, Subpart C.

QUESTION NO: 46

Which one of the following substances is not a hallucinogen?

A. Lysergic acid diethylamide

B. Mescaline

C. Phencyclidine

D. Phencyclidine analogs

E. None of the above

ANSWER: E

Explanation:

"None of the above" is correct because every substance named in the question is classified as a hallucinogen or hallucinogenic drug category member. Lysergic acid diethylamide and mescaline are classic psychedelics that can substantially alter perception, sensory experience, thought, and mood. Phencyclidine is generally described pharmacologically as a dissociative anesthetic, but it is also included in law-enforcement and drug-education classifications of hallucinogens because it can produce hallucinations, distorted perception, dissociation, and other profound changes in consciousness. Phencyclidine analogs, which are chemically related compounds, may likewise produce dissociative and hallucinogenic effects and are treated within the same general drug category for this type of classification question. Therefore, there is no listed substance that falls outside the hallucinogen category. This terminology is consistent with the U.S. Drug Enforcement Administration's overview of hallucinogens, which identifies LSD, mescaline, and PCP among relevant drugs, and the National Institute on Drug Abuse discussion of hallucinogenic and dissociative drugs.

QUESTION NO: 47

Top-guard supporting arms should be permanently affixed to the top of the fence 'posts to increase the overall height of the fence by at least:

A. 1 foot

B. 1 1/2 feet

C. 2 feet

D. 2 1/2 feet

E. 3 feet

ANSWER: A

Explanation:

1 foot is correct. Top-guard supporting arms are extensions installed securely on fence posts to support an outward-angled, inward-angled, or vertical top guard, commonly using strands of barbed wire or similar deterrent material. A minimum extension of 1 foot increases the effective height of the barrier and makes scaling more difficult by adding both physical reach and a visible psychological deterrent at the fence line. Permanently affixing the arms to the posts is important because the top guard must remain stable and continue to function as an integral part of the perimeter barrier under normal environmental conditions and attempted climbing or tampering.

This minimum reflects established physical-security fence design practice: the fence is evaluated as a system, including its fabric, posts, gates, foundations, clear zones, and top guard. The top guard is not merely an accessory; it contributes directly to delay by increasing the effort, time, and equipment an intruder needs to surmount the perimeter. Final top-guard configuration should also account for the site threat assessment, local codes, safety requirements, and the selected fence material. Guidance on security-fence planning and perimeter protective measures is available in the UFC 4-022-03 Security Fences and Gates and ASIS's security standards and guidelines resources.

QUESTION NO: 48

What type of fencing is generally used for protection of limited and exclusion areas?

A. Concertina

B. Barbed tape

C. Barbed wire

D. Chain-link

E. Wood

ANSWER: D

Explanation:

Chain-link is generally used to protect limited and exclusion areas because it provides a durable, clearly defined, and visible physical perimeter that can be installed at the required height and integrated with gates, locks, intrusion-detection systems, lighting, and surveillance. Its open mesh permits observation through the barrier, supporting guard-force assessment and camera coverage while still controlling access to a protected space. In higher-risk applications, chain-link fencing can be strengthened with top guards, barbed-wire or barbed-tape toppings, heavier fabric, and more robust posts; these are enhancements to the basic perimeter-fence system rather than a replacement for the primary fence type. This approach aligns with U.S. security-engineering guidance, which identifies chain-link fencing as a standard perimeter barrier and addresses its use with associated protective features. See the Department of Defense Unified Facilities Criteria for security fences and gates and the Whole Building Design Guide's perimeter security guidance. Thus, chain-link fencing is the general-purpose fencing selection for establishing the controlled boundary of limited and exclusion areas.

QUESTION NO: 49

Which of the following best describes an auditor's function?

A. Identify vulnerabilities, perform system tests, present reports

B. Analyze facts, draw conclusions, make recommendations

C. Configure systems, test alarms, create reports

D. Find weaknesses, develop equipment needs list, schedule installations

ANSWER: B

Explanation:

An auditor's function is best described as to **analyze facts, draw conclusions, make recommendations**. Auditing is an independent and systematic process of obtaining and evaluating objective evidence against defined criteria, such as policies, procedures, legal requirements, contractual obligations, or recognized standards. The auditor collects relevant evidence through document review, interviews, observation, testing, and sampling; evaluates whether the evidence demonstrates conformity and effective control operation; and communicates reasoned findings to management or other stakeholders. A useful audit does more than identify conditions: it presents conclusions supported by evidence and recommends practical corrective actions or improvements that help manage risk, strengthen governance, improve compliance, and enhance operational effectiveness. In a protection-program context, this may include evaluating whether

security controls are appropriately designed, implemented, maintained, and aligned with organizational objectives. The auditor remains objective and does not assume responsibility for operating or installing the controls being audited. This role is consistent with ISO's auditing guidance, which describes audit activities as gathering and evaluating objective evidence against audit criteria, and with The Institute of Internal Auditors' definition of internal auditing as providing assurance, advice, and insight to improve an organization's operations. See ISO 19011 auditing guidance and The IIA: What Is Internal Auditing?.

QUESTION NO: 50

In order to enforce compliance with safety and health standards under OSHA, employees are:

A. Required to comply within 5 days of written notice

B. Required to pay $10,000 per day for each day of noncompliance

C. Required to comply or to forfeit job

D. All of the above

E. None of the above

ANSWER: E

Explanation:

None of the above is correct because OSHA's enforcement mechanisms principally apply to employers, who have the legal duty to provide employment and a workplace free from recognized serious hazards and to comply with OSHA standards. When OSHA identifies violations, it may issue citations to the employer, establish an abatement deadline appropriate to the hazard and corrective action required, and propose penalties under the Occupational Safety and Health Act. The deadline is not universally five days, and monetary penalties are assessed against employers rather than employees. OSHA also protects workers who exercise safety and health rights, including reporting hazards or participating in inspections; workers may not lawfully be retaliated against for engaging in protected activity. Thus, the listed statements do not accurately describe a general OSHA requirement imposed on employees for enforcement purposes. The relevant statutory employer duty is found in Section 5 of the Act, while OSHA's overview of the citation-and-penalty process explains how violations are enforced. See OSHA: Section 5—Duties and OSHA: Penalties.

QUESTION NO: 51

Which security program emphasizes a continuing attitude that can move an individual to take specific actions to report or decrease security risks?

A. Training

B. Sustainment

C. Education

D. Awareness

ANSWER: D

Explanation:

Awareness is correct because a security awareness program is intended to develop and sustain an ongoing security-minded attitude among personnel. Its purpose extends beyond simply communicating information: it encourages people to recognize risks in their daily environment and respond constructively, such as by reporting suspicious activity, following protective procedures, or taking reasonable steps to reduce exposure to security threats. In an enterprise security program, awareness supports a positive security culture by making security a shared responsibility rather than the sole function of the security department. Effective awareness efforts are continuous and reinforced through regular communications, targeted campaigns, visible leadership support, and timely reminders tied to relevant threats or organizational risks. This continuing

emphasis helps translate security expectations into routine individual behavior and promotes early reporting, which allows the organization to assess and address issues before they escalate. ASIS guidance on developing security programs recognizes the importance of engaging personnel in the protection of organizational assets and operations. Additional security-awareness implementation guidance is available from the Cybersecurity and Infrastructure Security Agency and in NIST's Building an Information Technology Security Awareness and Training Program.

QUESTION NO: 52

Hallcrest I stated that the major item conspicuously absent from police-based crime prevention programs was:

A. A comprehensive training program

B. Manpower dedicated to crime prevention concepts

C. The input of a huge number of persons employed in private security

D. The use of updated technology

ANSWER: C

Explanation:

The input of a huge number of persons employed in private security is correct. The Hallcrest Report emphasized that private security personnel substantially outnumbered public law-enforcement personnel and represented a major, underused resource for preventing crime. Its central observation was that police-centered prevention efforts had generally not incorporated the knowledge, presence, observations, and preventive capabilities of the large private-security workforce. This workforce includes security officers and other private-sector personnel whose routine duties place them in positions to identify vulnerabilities, observe suspicious activity, deter criminal behavior, report incidents, and support coordinated prevention measures.

For protection professionals, the point is that effective crime prevention is not solely a police function. It depends on structured public-private cooperation, including information sharing, communication channels, defined responsibilities, and coordinated prevention initiatives. Incorporating private-security resources expands situational awareness and can improve the reach of preventive activity across commercial, institutional, residential, and public settings. The Hallcrest findings remain important context for modern security practice because they frame private security as an essential partner in the broader prevention system, rather than merely a separate response capability. See the Hallcrest Report I and the U.S. Department of Justice's Private Security and Public Policing.

QUESTION NO: 53

In substance a crime is;

A. A violent act

B. A violation of one's property

C. An act or omission prohibited by law that provides a punishment

D. A public wrong

E. A private wrong

ANSWER: D

Explanation:

A public wrong is correct because crime is fundamentally an offense against the public order and the state, rather than solely a dispute between private individuals. Criminal laws are enacted to protect the community's safety, security, welfare, and orderly functioning. When a person commits a crime, the conduct is treated as injuring society as a whole, which is why the government has authority to investigate, charge, and prosecute the alleged offender. The case is ordinarily brought in the name of the state or government, even when an identifiable individual has suffered direct harm.

This public character distinguishes criminal wrongdoing in substance: enforcement serves broader societal interests such as deterrence, accountability, incapacitation where appropriate, and maintenance of public peace. The Legal Information Institute describes criminal law as the body of law concerned with crimes and their punishment, while its discussion of public wrongs reflects the state's role in addressing conduct that harms the public. See Cornell Law School's Criminal Law overview and Cornell Law School's definition of crime.

QUESTION NO: 54

The purpose of formulating a civil disorder plan is to:

A. Ensure the safety and well-being of all personnel

B. Ensure full protection of company property

C. Ensure the continued operation of the facility

D. Help bring about a peaceful solution of the community problem

E. All of the above

ANSWER: E

Explanation:

All of the above is correct because an effective civil disorder plan uses an integrated, life-safety-first approach while also protecting organizational assets, sustaining essential operations, and supporting de-escalation. The plan should establish procedures to account for and protect employees, visitors, contractors, and responders; communicate protective actions; and coordinate evacuation, sheltering, access control, and medical support. It should also define proportionate measures to safeguard facilities, information, equipment, and other critical property without displacing the overriding priority of human safety.

Civil disorder can interrupt staffing, transportation, utilities, supply chains, and access to a site. Accordingly, planning must identify mission-essential functions, decision authorities, alternate work arrangements, communications, and recovery actions that enable the facility to continue operating at an appropriate level. Finally, security's role includes maintaining liaison and clear communication with public safety agencies and community stakeholders, using calm and lawful practices that reduce escalation and support a peaceful resolution. This aligns with emergency-planning principles that emphasize protecting people, maintaining critical functions, and coordinating incident actions. See OSHA's Emergency Action Plan guidance and FEMA's National Preparedness Goal.

QUESTION NO: 55

A fire involving ordinary combustible materials such as wastepaper and rags would be classified as:

A. Class A

B. Class B

C. Class C

D. Class D

E. Class E

ANSWER: A

Explanation:

Class A is correct because it covers fires involving ordinary combustible solids, including materials such as paper, wood, cloth, rubber, and many plastics. Wastepaper and rags are common examples of these fibrous, carbon-containing materials. Class A fires commonly leave ash after combustion and are typically controlled by cooling the burning material below its ignition temperature, most often with water when it is safe and appropriate to do so. Accurate fire classification is important

for security and facility-protection personnel because it supports selection of suitable extinguishing media, emergency procedures, and staff training. The Occupational Safety and Health Administration identifies Class A fires as those involving ordinary combustible materials, including wood, paper, and cloth. The National Fire Protection Association likewise uses Class A for ordinary combustibles in its portable fire-extinguisher classification system. See OSHA's fire prevention guidance and NFPA's fire extinguisher safety information.

QUESTION NO: 56

After the disaster plan has been fully prepared and tested, you as the security manager must make certain that the employees thoroughly understand it and actually take an active interest in it. Which of the following should not be done in your program of informing and educating the employees as to the plan?

A. Information disseminated to management should be prepared no differently from that contained in a general employee announcement.

B. Safety committees playa very important role in the development of the emergency plan.

C. Daily newsletters, bulletins, postings, and sales magazines should be closely evaluated as possible channels for the dissemination of disaster information.

D. New employees should be made aware of the existence of the disaster plan as soon as they come on duty.

E. Supervisory personnel are considered spokesmen for the company and employees naturally turn to these individuals for information.

ANSWER: A

Explanation:

"Information disseminated to management should be prepared no differently from that contained in a general employee announcement." is the action that should not be taken. Although all personnel need clear, accessible information about emergency procedures, management requires communications tailored to its distinct responsibilities. Leaders may need to understand activation authorities, incident-management roles, resource allocation, continuity priorities, escalation thresholds, communications with external agencies, and decisions necessary to protect people and sustain essential operations. A general employee announcement is appropriately focused on individual protective actions, reporting routes, evacuation or shelter instructions, and where to obtain further information; it is not sufficient preparation for personnel who must direct, coordinate, or make decisions during an incident.

Effective emergency planning therefore uses role-based training and communications. Management should receive information that enables it to execute assigned responsibilities and support the plan's command, control, and recovery processes. This approach also helps ensure that decisions made during a crisis are consistent with the tested plan rather than improvised. OSHA requires employers to review emergency action plans with employees when the plan is developed or changed and when employees' responsibilities change, reinforcing the importance of communicating responsibilities relevant to each person's role. See OSHA Emergency Action Plans, 29 CFR 1910.38 and FEMA Comprehensive Preparedness Guide 101.

QUESTION NO: 57

Which of the following is not an approved UL safe classification?

A. 350-1

B. 350-2

C. 350-3

D. 350-4

E. None of the above

ANSWER: E

Explanation:

None of the above is correct because each listed numerical designation corresponds to a recognized UL Class 350 fire-resistance duration rating for record-protection equipment. UL Class 350 ratings are intended for equipment that protects paper records by limiting the internal temperature during a prescribed fire-endurance test. The “350” designation identifies the maximum internal temperature criterion of 350°F (177°C), while the number after the hyphen denotes the fire-test duration in hours. Thus, one-hour, two-hour, three-hour, and four-hour Class 350 classifications are all valid classifications. UL also recognizes a one-half-hour Class 350 duration, although it is not included in this question. These fire classifications concern protection against heat exposure and should be distinguished from burglary-resistance ratings, which use separate designations such as TL-15 or TL-30. UL’s UL 72 standard listing identifies the governing standard for tests of fire resistance of record-protection equipment. Additional information on locating and verifying UL-certified products is available through UL Product iQ. Because every numbered Class 350 designation presented is an approved type of UL fire classification, no individual numbered entry satisfies the question’s request.

QUESTION NO: 58

The XYZ Manufacturing Plant Distribution Warehouse was destroyed in a fire. The Plant's emergency plan includes an agreement with a neighboring factory for use of their warehouse. This is an example of:

A. supply chain management.

B. mutual aid association.

C. emergency response agency.

D. business support network.

ANSWER: B

Explanation:

mutual aid association. is correct because the arrangement is established in advance between neighboring organizations so that one can provide a critical resource—the use of warehouse space—when the other suffers a disruptive loss. This type of reciprocal preparedness arrangement supports continuity of operations by identifying alternate facilities and defining how assistance will be provided before an incident occurs. In a manufacturing and distribution environment, promptly securing substitute storage or distribution capacity can reduce interruption, protect inventory flows, and support recovery objectives after a fire or other major event.

Mutual-aid arrangements are an important component of emergency preparedness and business continuity planning because they coordinate resources that may not be practical for every organization to maintain independently. Effective arrangements document the scope of available support, activation authority, access procedures, duration, costs, liability, security requirements, and communications. The agreement described is specifically a cooperative, preincident resource-sharing relationship, which is the essential characteristic of a mutual aid association. FEMA describes mutual aid as assistance provided between organizations through prearranged agreements, including the sharing of facilities and other resources. See FEMA’s Mutual Aid Agreements guide and ASIS’s security standards and guidelines resources.

QUESTION NO: 59

Which of the following is one step in the risk assessment process for use in protecting information?

A. Securing physical trade secret information

B. Providing ongoing security training information to employees

C. Identifying information assets

D. Confining intellectual knowledge of information

ANSWER: C

Explanation:

Identifying information assets is a foundational step in an information-protection risk assessment. Before an organization can evaluate risk, it needs a clear inventory of the information it owns, uses, stores, or transmits and an understanding of where that information resides. Information assets can include personally identifiable information, customer and employee records, intellectual property, trade secrets, financial data, system configurations, and sensitive business records. Asset identification establishes the scope for subsequent assessment activities, including identifying relevant threats and vulnerabilities, estimating likelihood and impact, determining risk levels, and selecting proportionate safeguards.

This activity also supports prioritization. Information does not have equal business value or require the same level of protection; identifying assets enables protection professionals to classify information according to sensitivity, criticality, legal or contractual requirements, and potential consequences of compromise. ISO/IEC 27001 treats an inventory of information and other associated assets as an important control for information-security management, while NIST risk-assessment guidance similarly begins by identifying the assets, systems, and information within the assessment scope. These practices allow security decisions to be based on documented business value and risk rather than assumptions. See ISO/IEC 27001 information-security management systems and NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

QUESTION NO: 60

An employer may not question an applicant about:

A. An unsatisfactory interview

B. Unexplained gaps in employment history

C. An arrest for a crime against property

D. A conviction for a crime against property

ANSWER: C

Explanation:

An arrest for a crime against property is the correct answer because an arrest does not establish that an applicant committed misconduct or was convicted of an offense. In employment screening, arrest information has limited probative value: a person may be arrested and released without charges, charges may be dismissed, or the person may be found not guilty. Consequently, using an arrest alone as a basis for an employment inquiry or decision can create unfair and potentially discriminatory screening practices.

For protection-professional hiring, screening must be relevant to the position, consistently applied, and compliant with applicable law. A lawful, job-related inquiry focuses on verified conduct or conviction information when it is relevant to the duties, risks, and trust placed in the position—not merely on an arrest record. The Equal Employment Opportunity Commission explains that an arrest alone does not establish criminal conduct and that employment decisions must be based on a legitimate, nondiscriminatory assessment of relevant information. See the EEOC's Enforcement Guidance on Arrest and Conviction Records and its guidance on background checks.

QUESTION NO: 61

The most important qualification of a good undercover operator is:

A. Resourcefulness

B. Education

C. Experience

D. Good contacts

E. None of the above

ANSWER: A

Explanation:

Resourcefulness is the most important qualification because undercover work is inherently dynamic: the operator must maintain a credible role while responding immediately and naturally to unexpected questions, changing conditions, and unplanned interactions. Resourcefulness combines practical judgment, adaptability, observation, initiative, and the ability to solve problems without drawing attention to the operation. These capabilities help the operator preserve cover, obtain reliable information lawfully, and make sound decisions when direct supervision or prearranged instructions cannot address the situation.

In a protection-investigation context, an undercover assignment must be carefully planned, authorized, and managed, but planning cannot eliminate uncertainty. A resourceful operator can adjust conduct and communications to the operational environment while remaining within the approved scope, applicable law, organizational policy, and ethical requirements. This competency is therefore central to both the effectiveness and safety of covert investigative activity. ASIS emphasizes that security professionals need sound judgment and practical application of investigative principles; see the ASIS Certified Protection Professional (CPP) certification overview and ASIS guidance on security standards and guidelines.

QUESTION NO: 62

One of the greatest hazards that would result from a nuclear attack is radioactive fallout.

A security manager should be well informed concerning the full potential of damage associated with this type of disaster. Which of the following is an incorrect statement?

A. Gamma radiation most concerns civil preparedness planners as it cannot be detected by any of the human senses.

B. Gamma radiation is measured in units called roentgens.

C. In an all-out nuclear attack against U.S. military, industrial, and population centers, it is estimated that severe to moderate damage from the blasts and heat effects would occur in about 50 percent of the nation's area.

D. Gamma radiation can be detected only with special instruments.

E. It is estimated that millions of Americans could survive the radiation effects of a large- scale nuclear attack by seeking protection in fallout shelters.

ANSWER: C

Explanation:

The statement that, in an all-out nuclear attack, severe to moderate blast and heat damage would occur in about 50 percent of the nation’s area is the incorrect statement. Blast overpressure and thermal effects are highly concentrated around individual detonation locations, and their geographic extent depends on such factors as weapon yield, burst altitude, terrain, and atmospheric conditions. Even a widespread attack against major military, industrial, and population targets would produce direct blast and thermal damage in discrete, heavily affected zones rather than across roughly half of the United States’ total land area. The far more geographically extensive hazard may be radioactive fallout, particularly downwind of ground bursts, because radioactive particles can be transported substantial distances by winds. Security planning must therefore distinguish between localized prompt effects—blast and heat—and the potentially broader but uneven distribution of fallout contamination. This distinction supports sound protective-action decisions, including sheltering, monitoring radiation conditions, and controlling access to contaminated areas. FEMA’s public guidance notes that fallout can be carried by winds and can affect areas far from the detonation site, while immediate destructive effects are centered near the explosion. See Ready.gov: Nuclear Explosion and CDC: Radiation Emergencies.

QUESTION NO: 63

Which of the following withdrawal characteristics can result from the abrupt cessation or reduction of high-dose depressant usage?

A. The withdrawal symptoms associated with depressants are more serious than those of any other drugs of abuse.

B. Convulsions can be experienced that are indistinguishable from those occurring in grand mal epilepsy.

C. Detoxification and treatment must be carried out under close medical supervision.

D. Both A and C.

E. All of the above.

ANSWER: E

Explanation:

"All of the above" is correct because abrupt cessation or a substantial dose reduction after high-dose central nervous system depressant use can produce a severe, potentially life-threatening withdrawal syndrome. This applies particularly to alcohol, barbiturates, and benzodiazepines, which reduce central nervous system activity; physiological dependence may develop with sustained use. When that depressant effect is suddenly removed, the nervous system can become dangerously overactive. Symptoms may include anxiety, tremor, autonomic instability, agitation, hallucinations, delirium, and seizures. Withdrawal seizures may be generalized tonic-clonic convulsions and can clinically resemble grand mal epileptic seizures. The risk is especially important in protection, workplace, and emergency-response contexts because affected individuals may deteriorate rapidly and require urgent medical assessment. Detoxification should therefore be medically managed, with clinicians able to monitor symptoms, address complications, and use an appropriate tapering or medication protocol rather than relying on abrupt discontinuation. The National Institute on Drug Abuse notes that withdrawal from benzodiazepines can include seizures and that medical supervision is important, while SAMHSA identifies alcohol withdrawal as a condition that may require medically supervised care. See NIDA's prescription-drug information and SAMHSA's treatment-support resources.

QUESTION NO: 64

Which of the following is not a requirement for handling preemployment interviews?

A. Interviews must be voluntary.

B. Interviews must be unbiased.

C. For an interview to be effective, it should be conducted with a witness or a friend of the applicant present.

D. The interviewer should not give out information.

E. Complete and accurate notes should be taken.

ANSWER: C

Explanation:

For an interview to be effective, it should be conducted with a witness or a friend of the applicant present is the correct choice because the presence of an applicant's friend is not a standard preemployment-interview requirement. Effective hiring interviews are normally structured, job-related conversations between the employer's authorized interviewer(s) and the applicant. An organization may choose to use a second company representative, such as a panel member or human-resources representative, for consistency, documentation, training, or corroboration. That is distinctly different from requiring an applicant to bring a friend or witness.

Sound preemployment interviewing practice focuses on a fair, consistent process that evaluates qualifications relevant to the position. Interviewers should use established questions and selection criteria, maintain appropriate records, and protect the integrity and confidentiality of the selection process. The U.S. Equal Employment Opportunity Commission explains that employment selection procedures must be administered without unlawful discrimination and should be related to the job. Its guidance is available at EEOC: Employment Tests and Selection Procedures. Practical guidance on structured interviews and consistent candidate evaluation is also available from the Society for Human Resource Management.

QUESTION NO: 65

An arrest made by a guard who has not been deputized is called:

A. A citizen's arrest

B. A conservator's arrest

C. An illegal arrest

D. A detention

E. None of the above

ANSWER: A

Explanation:

A citizen's arrest is correct because a security guard who has not been deputized or otherwise granted sworn peace-officer authority ordinarily acts as a private person rather than as a law-enforcement officer. In that capacity, the guard may possess the same limited arrest authority available to other citizens under the applicable jurisdiction's law. This authority is commonly described as a citizen's arrest, although its precise requirements—including whether the offense must occur in the person's presence and whether it must be a felony or breach of the peace—vary substantially by state or country.

For protection professionals, the practical point is that a nondeputized guard's authority is not created merely by the guard's employment title or uniform. The guard must understand the governing legal standard, use only reasonable force where permitted, promptly transfer the person to police custody, and document the facts supporting the action. Organizational policy, training, and legal counsel should address these jurisdiction-specific limits. Cornell Law School's Legal Information Institute describes citizen arrest in its legal reference materials at Citizen's arrest. The U.S. Department of Justice also provides criminal-justice resources relevant to law-enforcement practices at Office of Justice Programs.

QUESTION NO: 66

In issuing policy statements regarding the handling of disturbed persons, the primary consideration is:

A. Legal liability to the disturbed

B. Reducing the disturbed person to a form of benevolent custody and eliminating the immediate danger

C. Legal liability to employees and third persons if restraint is not achieved

D. Employee-community public relations

E. None of the above

ANSWER: B

Explanation:

Reducing the disturbed person to a form of benevolent custody and eliminating the immediate danger is the primary consideration because a response policy must first protect life and stabilize an unsafe situation. "Benevolent custody" describes taking protective control only to the extent necessary to prevent imminent harm, while preserving the individual's dignity and facilitating appropriate assistance. A sound policy therefore directs personnel to recognize signs of escalating behavior, use calm communication and de-escalation where feasible, summon trained supervisors, medical responders, or law enforcement as appropriate, and use the least restrictive safe intervention. The immediate objective is not punishment or resolution of every underlying issue; it is to prevent injury and move the person and those nearby to safety until qualified care or authority assumes responsibility.

This safety-centered approach is consistent with federal crisis-intervention guidance emphasizing de-escalation, assessment of immediate risk, and connection to appropriate emergency or behavioral-health resources. It also supports an organization's duty to establish procedures that help workers respond safely to threats and violence. See the U.S. Department of Justice's Crisis Intervention Team guide and OSHA's workplace violence resources.

QUESTION NO: 67

The acceptable vault construction of insulated doors has a minimum reinforced concrete wall, floor, and ceiling of:

A. 4 feet

B. 6 feet

C. 8 feet

D. 10 feet

E. 12 feet

F. 6 inches

ANSWER: F

Explanation:

The required minimum is **6 inches** of reinforced concrete for the vault's walls, floor, and ceiling. A vault is a complete protective enclosure, so the protective performance of the door assembly must be supported by continuous, comparably robust construction around every boundary of the protected space. Reinforced concrete at this minimum thickness provides a substantial delay barrier against forced entry while creating a structurally integrated enclosure that can properly support and secure a vault door and its locking hardware.

In security design, vault protection is evaluated as a system rather than as a door alone. The wall, floor, and ceiling construction must prevent an intruder from bypassing the door by attacking another surface or entering from an adjacent area. The stated six-inch minimum is therefore a thickness requirement, not a measurement in feet. Financial-institution security standards likewise address vault construction as a physical-security control and require consideration of vault integrity as part of a broader protective program. See the FDIC's security-device requirements in 12 CFR Part 326 and the GSA's physical-security guidance at GSA Building Security.

QUESTION NO: 68

A security manager is considering whether to outsource a guard-force function. Before making the decision, the manager should first determine:

A. The required service level, risks, and performance standards

B. The lowest available hourly billing rate

C. The number of local guard companies

D. The contractor's advertising budget

E. The preference of individual security officers

ANSWER: A

Explanation:

The required service level, risks, and performance standards is correct because outsourcing is a means of delivering a security service, not an objective in itself. Management must first define the posts, duties, response expectations, training requirements, supervision, reporting, technology interfaces, legal obligations, and performance measures necessary to manage the organization's risks. These requirements then provide a basis for evaluating whether internal staffing or a qualified contractor can deliver the service effectively and at an acceptable total cost.

Selecting a provider solely on hourly price can result in inadequate staffing, insufficient training, poor supervision, or contract terms that do not support the organization's security objectives. A well-developed scope of work and measurable service-level requirements support procurement, contract administration, and periodic performance review. See ASIS Standards and Guidelines.

QUESTION NO: 69

Rules promulgated by administrative agencies are ultimately published in the:

A. Code of Federal Regulations

B. U.S. Code

C. Federal Register

D. Statutes at large

E. Congressional Record

ANSWER: A

Explanation:

Code of Federal Regulations is correct because it is the official, subject-organized codification of federal administrative rules that are currently in force. When a federal agency completes the rulemaking process, the rule is initially issued through the Federal Register publication system. Once finalized and effective, it is incorporated into the Code of Federal Regulations, where regulations are arranged by subject into numbered titles and are available for ongoing reference and compliance use. This is the source security professionals commonly consult to identify operative federal regulatory requirements affecting such matters as workplace safety, transportation, environmental protection, privacy, and other regulated activities. The Code of Federal Regulations is updated through annual revisions and supporting update mechanisms to maintain an accessible compilation of current rules. The Office of the Federal Register describes the Code of Federal Regulations as the codification of the general and permanent rules published by executive departments and agencies. See the Government Publishing Office's Code of Federal Regulations collection and the National Archives overview of the Code of Federal Regulations.

QUESTION NO: 70

Perhaps one of the most difficult tasks in planning for disaster and emergencies is the actual formulation of a basic disaster plan. Which of the following is an incorrect procedure in developing such a plan?

A. The basic plan should provide for coordination of government and company actions before and during a disaster.

B. A glossary of terms used should be included.

C. There should be a listing of types of emergencies limited to those experienced by the company in the past.

D. The plan should utilize appendices as needed, such as maps, call-up lists, and mutual aid agreements.

E. The plan should specifically provide for coordination of government and company action before and during a disaster.

ANSWER: C

Explanation:

There should be a listing of types of emergencies limited to those experienced by the company in the past is the incorrect procedure because emergency and disaster planning must be based on a forward-looking, all-hazards risk assessment rather than an organization's loss history alone. Past incidents are useful inputs: they may reveal recurring vulnerabilities, response gaps, or likely operational impacts. However, they cannot reliably identify emerging, low-frequency/high-consequence, location-specific, supply-chain, technological, natural, or human-caused threats that have not yet occurred at the organization.

A sound basic disaster plan identifies hazards through systematic assessment of threats, vulnerabilities, likelihood, and potential consequences. It then establishes flexible capabilities that can be adapted to multiple scenarios, including events that have never previously affected the company. This approach supports continuity of critical operations, life safety, coordination with public authorities, communications, and recovery even when the precise initiating event differs from prior experience. FEMA's Comprehensive Preparedness Guide describes planning as a community-driven, risk-informed process that considers the full range of threats and hazards. FEMA's preparedness planning guidance is available at

https://www.fema.gov/emergency-managers/national-preparedness/plan and its Comprehensive Preparedness Guide 101 at https://www.fema.gov/sites/default/files/2020-05/CPG_101_V3.pdf.

QUESTION NO: 71

An indication of deception by a suspect during the interviewing process would be:

A. giving direct, spontaneous responses to questions.

B. asking clarifying questions

C. casually changing position.

D. engaging in a variety of tension-relieving gestures.

ANSWER: D

Explanation:

engaging in a variety of tension-relieving gestures. is the best indication because deception can create cognitive load, anxiety, and concern about being detected. A subject may attempt to manage that discomfort through adaptors or self-soothing behaviors, including repeated fidgeting, face touching, clothing adjustment, hand wringing, or frequent shifts in posture. A variety and increase of such gestures during material questions can be a useful behavioral cue for an interviewer to explore further.

Professional interviewing practice requires the interviewer to establish the person's normal behavioral baseline early in the conversation and then assess meaningful changes in behavior in relation to specific topics or questions. Tension-relieving gestures are not proof of dishonesty by themselves: they are an investigative lead that should prompt neutral follow-up questions and corroboration through facts, records, and other evidence. This contextual approach is consistent with the behavioral-observation and investigative-interviewing knowledge expected of protection professionals. ASIS describes the CPP credential's broad security-management body of knowledge at ASIS CPP certification. Guidance on evidence-based interviewing and the limits of behavioral deception detection is also available from the National Institute of Justice.

QUESTION NO: 72

The OSHA Act allows states to continue their present safety and health enforcement activities provided that:

A. The state program is "at least as effective" as the federal program

B. The Secretary of Labor signs a certificate of authorization

C. The attorney general after hearing approves

D. Litigation is pursued in the federal court system

E. None of the above

ANSWER: A

Explanation:

The state program is "at least as effective" as the federal program. Section 18 of the Occupational Safety and Health Act permits a state to assume responsibility for occupational safety and health standards and enforcement through an OSHA-approved State Plan. A central statutory requirement is that the state plan provide standards and enforcement that are, or will be, at least as effective as the federal program in preventing workplace injuries, illnesses, and fatalities. This requirement is substantive: the state must have adequate legal authority, enforcement procedures, qualified personnel, inspection capability, and penalty mechanisms to deliver protection comparable to federal OSHA. State programs may tailor rules and operations to local industries and conditions, but their overall worker-protection results and enforcement capacity must meet the federal effectiveness threshold. OSHA monitors approved plans and may withdraw approval if a state no longer maintains an effective program. This federal-state structure preserves a national baseline for employee safety while allowing

states to administer their own programs. See OSHA's overview of State Plans and the statutory requirements in 29 U.S.C. § 667.

QUESTION NO: 73

If the interviewee during an investigation is hostile, it is preferable to conduct the interview at:

A. The security office

B. The home of the interviewee

C. A neutral spot

D. In an automobile

E. At the office of the interviewee's lawyer

ANSWER: A

Explanation:

The security office is the preferable setting because a hostile interviewee should be met in a location that is controlled, professional, private, and suitable for safely managing the interaction. A security office typically provides the investigator with access to appropriate documentation, communication resources, and assistance if needed, while reducing interruptions and limiting the interviewee's ability to control the environment. It also supports orderly preparation, observation, and documentation of the interview. The setting should be arranged to preserve the interviewee's dignity and to avoid unnecessary intimidation; the goal is to establish appropriate control and safety, not to coerce a statement. Investigators must remain alert to legal requirements, organizational policy, and the voluntary nature of a noncustodial interview, including ending or pausing the interview if safety concerns arise. This approach is consistent with professional security-management practice emphasizing planned investigations, suitable interview conditions, and effective incident management. ASIS provides professional guidance and standards resources for security management at ASIS Standards & Guidelines. The U.S. Department of Justice also emphasizes structured, professional investigative interviewing practices in its National Institute of Justice interviewing guide.

QUESTION NO: 74

Once published, an emergency plan for disaster control should be distributed:

A. On a need-to-know basis

B. Only to the highest echelon

C. Only to division heads

D. Down to the lowest echelons assigned responsibility

E. To none of the above

ANSWER: D

Explanation:

"Down to the lowest echelons assigned responsibility" is correct because an emergency or disaster-control plan is operational only when every person who has a defined response duty can access, understand, and apply the procedures relevant to that duty. Distribution must therefore reach all assigned levels of the organization, including personnel responsible for initial notification, evacuation support, accountability, communications, shutdown activities, access control, first aid, and recovery coordination. This ensures that authority, reporting relationships, actions, and resource requirements are understood before an incident occurs rather than being improvised during a crisis.

Effective plan distribution is also paired with orientation, training, exercises, and periodic updates. Personnel need current copies or reliable access to the portions of the plan that govern their responsibilities, while controlled distribution methods

can protect sensitive information without preventing responsible staff from performing their roles. FEMA's planning guidance emphasizes assigning responsibilities and communicating the plan to those who must implement it. OSHA likewise requires employers to establish and communicate emergency-action procedures to employees. See FEMA Comprehensive Preparedness Guide 101 and OSHA Emergency Action Plans, 29 CFR 1910.38.

QUESTION NO: 75

Approximately what percentage of medium and large security departments deputize private security personnel or give them special police powers?

A. 10 percent

B. 25 percent

C. 50 percent

D. 60 percent

ANSWER: B

Explanation:

25 percent is the correct approximate figure. This statistic reflects the limited, jurisdiction-dependent use of delegated public-law-enforcement authority by private-security organizations. In medium and large security departments, a meaningful minority of personnel may receive deputization or specially authorized police powers, typically to support protection duties at locations such as campuses, transportation facilities, public authorities, or other properties where governing law permits a defined grant of authority. The figure does not mean that private-security personnel broadly possess the same authority as public police officers. Rather, any special authority is derived from applicable legislation, appointment procedures, and the terms imposed by the relevant public agency or jurisdiction. CPP candidates should distinguish ordinary private-security functions—such as observing, reporting, access control, and protecting property—from authority that is formally delegated and legally bounded. The approximate 25-percent figure is therefore a useful benchmark for recognizing that deputization exists in a substantial but nonmajority share of larger security operations. For broader context on the statutory regulation and public-safety role of private security, see the U.S. Bureau of Justice Statistics report on private security and ASIS International's standards and guidelines resources.

QUESTION NO: 76

The sensor that is used when air turbulence is present in the room being protected and when there are no potential false alarm sources outside the room and in the field of the detector is a (n):

A. Vibration detector

B. Microwave motion detector

C. Ultrasonic motion detector

D. Acoustic detector

E. None of the above

ANSWER: B

Explanation:

Microwave motion detector is correct because it detects movement by transmitting microwave energy and evaluating changes in the reflected signal caused by a moving person or object. Unlike ultrasonic volumetric detection, its detection performance is not dependent on stable air movement patterns within the protected space. This makes microwave sensing an appropriate selection where air turbulence from HVAC systems, fans, or drafts is expected.

Microwave energy can extend beyond the intended protected area, including through some nonmetallic building materials, depending on the detector's frequency, power, mounting, and site conditions. The stated condition that there are no potential

false-alarm sources outside the room and within the detector's effective field is therefore essential to its suitable application. During design and commissioning, the protection professional should adjust the detector's range and aim, verify coverage by walk testing, and confirm that activity in adjacent areas cannot produce an alarm. This reflects the broader CPP expectation that intrusion-detection technologies be selected and configured according to environmental conditions and the protected asset's risk profile. See ASIS's Certified Protection Professional overview and Bosch's microwave detector technical documentation for related detector characteristics.

QUESTION NO: 77

Theft involves the crime of:

A. Robbery

B. Embezzlement

C. Larceny

D. False pretenses

E. All of the above

ANSWER: E

Explanation:

All of the above is correct because theft is a broad term for offenses involving the unlawful taking, obtaining, or conversion of another person's property with the required criminal intent. In traditional criminal-law terminology, larceny is the trespassory taking and carrying away of personal property; embezzlement concerns the fraudulent conversion of property by someone who was entrusted with or lawfully possessed it; and false pretenses involves obtaining title to property through a material misrepresentation. Robbery is also a theft-related offense, generally consisting of a taking of property from a person or their presence by force or threat of force. Although modern statutes often consolidate these historically distinct common-law property offenses under a single theft statute, security professionals should recognize each term because incident reporting, investigations, loss-prevention controls, and liaison with law enforcement may depend on the method by which property was unlawfully obtained. The Legal Information Institute describes theft as encompassing multiple property offenses and provides definitions of the related offenses, including theft and robbery.

QUESTION NO: 78

Which of the following is true with regard to the power of detention?

A. Detention differs from arrest.

B. It is lawful as long as it is for a reasonable time and conducted reasonably.

C. There is no one standard to apply.

D. All of the above.

E. None of the above.

ANSWER: D

Explanation:

All of the above is correct because the authority to detain is a limited, fact-dependent power rather than a universal authority to arrest. A detention generally means a temporary restriction of a person's freedom of movement for a specific lawful purpose, such as investigating a reasonable concern, determining whether an offense has occurred, or recovering property. It differs from an arrest, which ordinarily involves taking a person into custody under a greater level of legal authority and with more substantial consequences.

For security professionals, the central operational principle is reasonableness. The grounds for the detention, the manner in which personnel act, the degree of force used, the location, and the length of time must all be proportionate to the circumstances and consistent with applicable law and organizational policy. A person should be released or transferred promptly once the purpose of the detention has been resolved or law enforcement assumes control.

There is no single standard that applies everywhere because detention authority varies by jurisdiction, including statutes governing private persons, shopkeeper privileges, citizen arrest, and relevant case law. Security leaders should therefore establish procedures with qualified legal counsel and train personnel to document the factual basis and timing of every detention. See Cornell Law School's discussion of false imprisonment and the U.S. Supreme Court's decision in Terry v. Ohio.

QUESTION NO: 79

Knowing where security fits into a company's budget is critical to the manager successfully accessing financial resources. Which of the following statements best describes a security department's impact on the bottom line?

A. The security department's costs must be minimized to reduce the expense side of the corporate ledger

B. The security department is an investment with a predictable rate of return.

C. The security department's expense requests must be supported by a cost-benefit analysis.

D. The security department helps the profit margin by reducing or preventing losses of company assets.

ANSWER: D

Explanation:

The security department helps the profit margin by reducing or preventing losses of company assets. This accurately characterizes security as a business function that protects organizational value, rather than merely as an overhead expense. Effective security programs identify, assess, and treat risks that could produce direct or indirect financial loss, including theft, fraud, property damage, business interruption, liability, and loss of information or other assets. Avoiding or reducing the frequency and severity of these events preserves assets and revenue, limits unplanned costs, and supports continuity of operations. Those avoided losses can improve the organization's financial performance and protect its profit margin. In CPP practice, security leaders communicate this contribution in business terms by connecting security measures to risk reduction, asset protection, and organizational objectives. The precise financial return from a particular safeguard may not always be predictable, but the department's fundamental bottom-line contribution is reducing the losses that would otherwise diminish profitability. This approach is consistent with risk-management principles: the value of controls is evaluated in relation to the risk they mitigate and the consequences they help avoid. See ASIS International's CPP certification overview and ISO 31000 risk management guidance.

QUESTION NO: 80

The release of a convicted person under certain conditions without having to be imprisoned is known as:

A. Probation

B. Parole

C. Corpus juris

D. Detainer

E. Commutation

ANSWER: A

Explanation:

Probation is correct because it is a court-imposed sentencing disposition that permits a person convicted of an offense to remain in the community rather than serve a term of incarceration, provided that the person complies with specified

conditions. Those conditions are tailored by the sentencing court and may include regular reporting to a probation officer, maintaining employment, obeying laws, attending treatment or counseling, paying restitution, avoiding certain people or places, and submitting to testing when ordered. The essential feature in the question is that the convicted person is allowed to avoid imprisonment subject to conditions and supervision. Probation can be imposed as the primary sentence, and courts may also impose a period of probation following a limited custodial sentence where authorized by law. Failure to comply can result in a violation proceeding and potentially more restrictive sanctions, including incarceration. The federal judiciary describes probation officers' role in supervising people sentenced to probation and helping courts monitor compliance with judicial conditions. See the U.S. Courts Probation and Pretrial Services overview. For the statutory federal framework governing probation conditions and supervision, see 18 U.S.C. § 3563.

QUESTION NO: 81

Which type of alarm sensor detects heat from a human body?

A. Microwave

B. Passive infrared

C. Temperature

D. Ultrasonic

ANSWER: B

Explanation:

Passive infrared is correct because a passive infrared sensor detects naturally occurring infrared energy radiated by objects within its field of view, including the thermal energy emitted by the human body. In intrusion detection applications, the sensor does not measure a person's temperature as a thermometer would. Instead, its pyroelectric sensing element responds to a change in the infrared pattern reaching the detector. When a person moves across the detection zones created by the sensor's optics, the changing contrast between the person's heat signature and the background produces an electrical signal that can initiate an alarm.

The term "passive" is important: the device does not transmit energy into the protected space. It receives infrared radiation already present in the environment. This operating principle makes passive infrared detection particularly useful for interior motion detection, where coverage, mounting location, background thermal conditions, and expected direction of travel should be considered during design and installation. Manufacturer technical guidance describes PIR detectors as sensing changes in infrared radiation caused by moving people or other warm objects. See Bosch Security motion detector information and Axis Communications' thermal-imaging technology overview.

QUESTION NO: 82

The condition whereby a user must keep increasing the dosage to maintain the same effect is known as:

A. Tolerance

B. Addiction

C. Psychological dependence

D. Physical dependence

E. Habituation

ANSWER: A

Explanation:

Tolerance is the correct term for the reduced response to a drug or other substance after repeated use, such that a person requires progressively larger doses to achieve the effect that was previously obtained with a smaller dose. It can develop with many substances, including alcohol, opioids, sedatives, and stimulants. In a protection-management context, accurately

distinguishing tolerance from substance-use disorder concepts is important when recognizing potential impairment, communicating concerns, and applying workplace policies consistently and appropriately. Tolerance is a physiological or pharmacological adaptation; it may occur during ongoing use but does not, by itself, establish that an individual has a substance use disorder. The U.S. National Institute on Drug Abuse describes tolerance as needing larger amounts of a drug to obtain the same effect, and the National Institute on Alcohol Abuse and Alcoholism similarly identifies it as a possible feature considered in alcohol use disorder assessment. See the National Institute on Drug Abuse overview of drug misuse and addiction and the National Institute on Alcohol Abuse and Alcoholism explanation of alcohol use disorder.

QUESTION NO: 83

Information that could lead to the compromise of vital national defense plans or complex cryptologic and communications intelligence systems should be classified:

A. Restricted

B. Secret

C. Confidential

D. Top secret

E. Cosmic

ANSWER: D

Explanation:

Top secret is the appropriate classification because U.S. national-security classification standards reserve this level for information whose unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to national security. Examples expressly associated with this threshold include the compromise of vital national defense plans and complex cryptologic or communications intelligence systems. These types of information can expose critical military capabilities, intelligence sources and methods, command-and-control arrangements, or national-level operational plans. The likely consequences therefore extend beyond localized or serious harm and can affect the nation's ability to defend itself, protect strategic operations, and preserve highly sensitive intelligence advantages.

For protection professionals, the classification indicates that the information requires the most stringent safeguards: access is limited to personnel with an appropriate clearance, a verified need to know, and compliance with approved handling, storage, transmission, and destruction controls. The classification decision must be made through authorized original or derivative classification processes and documented in accordance with applicable government policy. Executive Order 13526 defines the "exceptionally grave damage" standard for Top Secret information, while the Information Security Oversight Office provides the federal classification framework and oversight resources. See Executive Order 13526 and the Information Security Oversight Office.

QUESTION NO: 84

A psychopath can often pass a polygraph test with a clean record because of the following characteristic:

A. Uncooperative attitude

B. Unstable personality

C. An inferiority complex

D. An abnormal lack of fear

E. Both B and C

F. All of the above

ANSWER: D

Explanation:

An abnormal lack of fear is correct because polygraph examinations infer possible deception from physiological activity, such as changes in respiration, sweating (electrodermal activity), and cardiovascular responses, during relevant questioning. A core feature often associated with psychopathy is reduced fearfulness and diminished autonomic reactivity to threatening, stressful, or punishment-related stimuli. If an examinee experiences comparatively little fear, anxiety, or anticipatory stress while answering deceptive questions, the physiological changes on which a polygraph relies may be less pronounced or less discriminable. This can make a deceptive response more difficult to distinguish from the person's baseline response pattern.

For protection professionals, the key point is that a polygraph is not a direct detector of lies and should not be treated as conclusive evidence of truthfulness or deception. Its output reflects physiological measurements that can be influenced by individual differences in emotional responsiveness, psychological condition, examination context, and countermeasures. The National Research Council's review discusses the limitations of polygraph validity and the importance of physiological-response variability. Research on psychopathy likewise identifies low fear and atypical defensive responding as relevant characteristics. See the National Research Council's Polygraph and Lie Detection report and research on psychopathy and fear-potentiated startle.

QUESTION NO: 85

An example of a mala prohibitum crime is:

A. Rape

B. Illegal parking

C. Murder

D. Kidnapping

E. Assault

ANSWER: B

Explanation:

Illegal parking is correct because it is an offense that is unlawful primarily because a statute, ordinance, or regulation prohibits it. This is the defining feature of *mala prohibita*: conduct becomes criminal through a legislative or regulatory determination intended to support public order, safety, and efficient administration. Parking restrictions, for example, can preserve traffic flow, maintain emergency access, protect accessible parking spaces, and facilitate the orderly use of limited public space. The conduct itself is not inherently or universally immoral; its criminal or civil-offense character depends on the applicable rule and jurisdiction.

In protection-management practice, distinguishing offenses that are prohibited by regulation from inherently wrongful acts helps security professionals understand the nature of an incident, applicable policies, enforcement authority, and appropriate escalation or reporting processes. A parking violation may require notice, citation, towing, or coordination with public authorities according to site policy and local law. Legal-reference materials commonly describe *malum prohibitum* as an act made unlawful by statute rather than by its intrinsic nature. See Cornell Law School's definition of malum prohibitum and the Legal Information Institute's overview of parking law.

QUESTION NO: 86

Which of the following factors should be evaluated in considering the need for security officers to have weapons?

A. The type of encounter to be faced by the security officer

B. The nature of the potential threat

C. The operational objective of the security officer

D. All of the above

E. None of the above

ANSWER: D

Explanation:

All of the above is correct because a decision to arm security officers must be based on a documented, risk-based assessment rather than a single condition. The type of encounter officers may face matters because responsibilities can range from routine access control and customer interaction to intervention in potentially violent incidents. The nature of the potential threat must be evaluated, including the likelihood, capability, intent, and consequences associated with violence or weapons at the protected location. The operational objective also matters: an officer assigned principally to observe, deter, report, and summon law enforcement may require a different capability and response model than one expected to protect people during high-risk operations or to respond immediately to violent threats.

ASIS security-management guidance emphasizes tailoring protective measures to the organization's risk environment, mission, and operational requirements. An armed-officer program should therefore also be supported by lawful authority, clearly defined post orders and use-of-force policy, careful selection, initial and recurrent training, supervision, safe weapons controls, and coordination with public law enforcement. These considerations help ensure that any weapons decision is proportionate to the risks and compatible with the officer role. See ASIS International's standards and guidelines resources and OSHA's workplace violence prevention guidance.

QUESTION NO: 87

A small hidden microphone and a radio transmitter are generally known as:

A. A wiretap

B. A bug

C. A beeper

D. Electronic surveillance

E. All of the above

ANSWER: B

Explanation:

A bug is the generally accepted term for a covert electronic listening device that combines a small microphone with a transmitter. The microphone captures nearby speech or sound, and the transmitter sends the audio signal—typically by radio frequency—to a receiver where it can be monitored or recorded. In security and counter-surveillance contexts, "bug" is commonly used to describe a concealed audio-surveillance device placed in a room, vehicle, office fixture, telephone, or other location. This terminology is also reflected in U.S. legal language addressing the interception of oral communications through electronic, mechanical, or other devices. Security professionals need to recognize such devices as a technical-surveillance threat and address them through appropriate technical surveillance countermeasures, physical-security controls, inspection procedures, and incident-response processes. The U.S. Department of Justice discusses electronic surveillance and interception authorities at https://www.justice.gov/archives/jm/criminal-resource-manual-1052-electronic-surveillance. For statutory terminology concerning devices used to intercept oral communications, see the Legal Information Institute's text of 18 U.S.C. § 2510 at https://www.law.cornell.edu/uscode/text/18/2510.

QUESTION NO: 88

A type of bodily disability wherein a person unconsciously converts his or her anxiety into a strong belief that some part of his or her body has ceased to function is:

A. Malingering

B. Hysterics

C. Conversion hysteria

D. Depression

E. Phobia

ANSWER: C

Explanation:

Conversion hysteria is the correct answer. This older term refers to what modern diagnostic terminology generally calls conversion disorder, or functional neurological symptom disorder. It involves the unconscious expression of psychological conflict, stress, or anxiety as neurological-like physical symptoms, such as weakness, paralysis, loss of sensation, impaired speech, tremor, or non-epileptic seizures. The symptoms are experienced as real by the individual and are not intentionally produced. In the wording of the question, anxiety is converted into a perceived loss of bodily function; that description directly reflects the classic concept of conversion hysteria.

For protection professionals, recognizing this concept supports appropriate, respectful handling of an individual who appears physically impaired or distressed. Personnel should treat reported symptoms seriously, avoid accusing the person of fabrication, protect the individual's safety, and obtain appropriate medical evaluation under organizational procedures. The current clinical description and diagnostic context for functional neurological symptom disorder are summarized by the Merck Manual and the National Institute of Neurological Disorders and Stroke.

QUESTION NO: 89

An employee ' s access to information should be based on what criteria?

A. Their knowledge of the subject matter.

B. Their position or management level.

C. Their current job function and " need-to-know. "

D. Their organizational relationship to the information owner.

ANSWER: C

Explanation:

Access based on "Their current job function and "need-to-know."" applies the foundational access-control concepts of least privilege and need-to-know. An employee should receive authorization only for the information resources required to carry out assigned, current duties. Job function provides the basis for defining an appropriate role or access profile, while need-to-know limits the scope of information within that role to a legitimate business requirement. This approach helps protect confidentiality by reducing unnecessary exposure of sensitive information, limits opportunities for misuse or accidental disclosure, and makes access reviews more meaningful when responsibilities change. In a protection program, the information owner and security function should establish classifications, role-based entitlements, approval procedures, and periodic reviews so that access remains aligned with the employee's present responsibilities—not merely title, seniority, expertise, or personal relationship to the owner. The same principle supports prompt removal or adjustment of permissions when an employee transfers, changes duties, or separates. NIST identifies least privilege as restricting access to the minimum necessary to accomplish authorized tasks, and ISO/IEC 27001 guidance addresses access-control rules based on business and information-security requirements. See NIST's definition of least privilege and ISO/IEC 27001 information security management standard.

QUESTION NO: 90

Capacitance alarm systems are sometimes referred to as:

A. sonic alarms.

B. proximity alarms.

C. vibration detector alarms.

D. ultrasonic alarms

ANSWER: B

Explanation:

proximity alarms. is correct because a capacitance alarm detects the approach or presence of a person or conductive object within an established electrostatic field. The protected conductor—such as a wire, screen, fence, or other sensing element—forms part of an electrical capacitance circuit. When a person approaches it, the person's body changes the capacitance of the circuit. If that change exceeds the system's programmed threshold, the alarm initiates.

The defining feature is therefore detection based on nearness to the sensing element rather than physical contact with it. "Proximity" accurately describes this detection method and is the terminology commonly used for capacitance-based perimeter and object-protection detection applications. The technology can be configured to protect items such as safes, cabinets, display cases, or restricted zones where an early warning before direct contact is valuable. Sound operational design includes appropriate sensitivity adjustment, environmental testing, grounding, and assessment of nearby conductive materials, all of which affect the protected field and nuisance-alarm resistance.

This terminology and the underlying need to select detection technologies according to the asset, threat, and operating environment align with the physical-security knowledge expected in the ASIS CPP certification domain. See ASIS Certified Protection Professional (CPP) and CISA physical security resources.

QUESTION NO: 91

A wooden plank-and-beam room used for secure storage has no windows or environmental controls. The room will experience a temperature of 98.6'F (37gC) for about 20 minutes at 11:23 A.M. and again at 8:17 P.M. for several months during the summer. Which sensor listed below would have its detection ability affected by this scenario?

A. Microwave sensor

B. Ultrasonic sensor

C. Photoelectric beam sensor

D. Passive infrared sensor

ANSWER: D

Explanation:

Passive infrared sensor is correct because this type of detector identifies motion by sensing a changing infrared-energy pattern across its detection zones. A person is normally distinguishable from the surrounding area because the person's skin and clothing produce a thermal signature that contrasts with ambient conditions. When the protected room reaches approximately normal human body temperature, that contrast is substantially reduced. An intruder moving through the room may therefore create a weaker infrared change at the detector, reducing detection reliability during those recurring high-temperature periods.

This is an important environmental-design consideration for interior intrusion detection. Detector selection and placement must account for expected ambient temperatures, seasonal heat buildup, direct or reflected heat sources, and the thermal characteristics of the protected space. In an unconditioned wooden storage room, repeated periods near body temperature can create predictable intervals in which a passive infrared device has diminished ability to discriminate a moving person from the background. Security practitioners should address this through suitable sensor technology, environmental mitigation, or layered detection appropriate to the assessed risk. The U.S. Department of Energy describes infrared sensing as detection of emitted heat energy, while the National Institute of Standards and Technology provides guidance on assessing and managing physical-security risks: U.S. Department of Energy—Infrared Thermography; NIST SP 800-53.

QUESTION NO: 92

Which of the following is not another name for a barbiturate?

A. Tuinal

B. Butisol

C. Phenobarbital

D. Amobarbital

E. Dilaudid

F. None of the above

ANSWER: E

Explanation:

Dilaudid is the correct answer because it is a brand name for hydromorphone, a potent opioid analgesic used to treat moderate to severe pain. Hydromorphone acts primarily as a mu-opioid receptor agonist and is classified as an opioid/narcotic analgesic, not as a barbiturate. Drug classification is important in protection, investigative, and workplace contexts because opioid effects, impairment indicators, overdose risks, regulatory controls, and diversion concerns differ substantially from those associated with sedative-hypnotic barbiturates. The U.S. National Library of Medicine's MedlinePlus identifies hydromorphone as an opioid analgesic and provides its prescribing and safety information. The U.S. Drug Enforcement Administration also categorizes hydromorphone as a Schedule II controlled substance under the Controlled Substances Act, reflecting its accepted medical use alongside a high potential for misuse and dependence. These authoritative classifications establish that Dilaudid is not a name for a barbiturate. See MedlinePlus: Hydromorphone and the DEA Controlled Substances list.

QUESTION NO: 93

Unless appealed, payment of penalties under OSHA must be made within:

A. 10 working days

B. 5 working days

C. 15 working days

D. 30 working days

E. 2 months

ANSWER: C

Explanation:

15 working days is correct. Under the Occupational Safety and Health Act, after an employer receives an OSHA citation and notification of proposed penalty, the employer has 15 working days to file a notice of intent to contest the citation, proposed penalty, or abatement period. If the employer does not contest within that statutory period, the citation and proposed penalty become a final order of the Occupational Safety and Health Review Commission by operation of law. The penalty is then due and payable.

This deadline is important for security and protection professionals because OSHA citations may arise from workplace hazards affecting employees, contractors, emergency procedures, or facility operations. Promptly routing a citation to appropriate legal, safety, finance, and executive stakeholders is necessary to determine whether a contest is warranted and to ensure timely payment when it is not. The 15-working-day period begins upon the employer's receipt of the citation and proposed penalty notification, rather than when the organization internally distributes or reviews the document. See Section 10(a) of the OSH Act at OSHA: Section 10—Procedure for Enforcement and OSHA's employer guidance at OSHA Employer Rights and Responsibilities Handbook.

QUESTION NO: 94

The decision whether to evacuate a building as a result of a bomb threat will be made by the:

A. FBI

B. Police

C. Management

D. Military

E. Employees' union

ANSWER: C

Explanation:

Management is correct because the organization that occupies or controls the facility retains responsibility for protecting its people, continuing essential operations where possible, and making timely life-safety decisions. In a bomb-threat incident, management—typically through a designated incident-management team, security leader, or senior executive—assesses the available information, the facility's emergency plan, operational requirements, and the potential consequences of evacuation or sheltering in place. The decision should be made within a pre-established emergency-management structure and communicated promptly through defined notification procedures.

Law-enforcement and bomb-squad personnel provide critical threat assessment, investigative support, and tactical recommendations. Their input helps management make an informed decision, particularly when there is specific information indicating a credible or imminent hazard. However, the facility's management has the primary duty to activate its emergency procedures and direct occupants unless public authorities assume control under applicable law or an immediate emergency requires responders to issue protective instructions. Effective bomb-threat planning therefore establishes decision authority in advance, identifies alternates, and ensures coordination with emergency services. Guidance on bomb-threat response and protective actions is available from CISA's Bomb Threats resources and Ready.gov's evacuation guidance.

QUESTION NO: 95

The most vulnerable link in any identification system is:

A. Poor quality of identification badges

B. Educational background of security officers

C. Not enough security officers assigned to control posts

D. Identification cards are too small

E. Perfunctory performance of duty

F. None of the above

ANSWER: E

Explanation:

Perfunctory performance of duty is the most vulnerable link in an identification system because identification controls ultimately depend on the person responsible for applying them consistently. Even well-designed badges, credential technologies, access procedures, and staffing plans can be defeated when personnel conduct only a superficial check, fail to compare the credential with the individual, overlook signs of alteration or misuse, permit tailgating, or make undocumented exceptions. Effective identification programs therefore require clear post orders, training on credential inspection and challenge procedures, supervisory observation, and routine testing of guard performance. Security management must ensure that officers understand both the purpose of identity verification and their authority to deny entry or escalate concerns. This reflects the broader protection principle that people and their execution of procedures are essential components of any physical security control; a credential is only meaningful when it is properly examined and enforced at the point of entry. ASIS guidance on physical security emphasizes the integration of personnel, procedures, and technology in access-control operations. See ASIS access-control resources and the CISA Physical Security Performance Goals for related guidance on implementing and sustaining access-control measures.

QUESTION NO: 96

During an emergency evacuation of a facility, special provisions must be made for:

A. securing vital business information

B. assisting disabled persons.

C. a muster point.

D. command and control.

ANSWER: B

Explanation:

Assisting disabled persons. is correct because an evacuation plan must account for people who may be unable to perceive an alarm, understand instructions, travel independently, use stairs, or move quickly to an exit. This includes individuals with mobility, sensory, cognitive, or temporary impairments, as well as visitors who may need assistance. Effective protective planning identifies these needs before an incident, assigns trained assistants or a buddy system where appropriate, establishes accessible evacuation routes and areas of refuge, and provides suitable equipment or procedures for safe egress. These provisions should be incorporated into emergency action planning, communicated to affected personnel, and tested through drills so that assistance is reliable under real emergency conditions. Life safety is the primary objective of evacuation, and inclusive planning helps ensure that all occupants have a practical means of reaching safety rather than relying on improvised assistance during a crisis. OSHA's emergency planning guidance specifically calls for procedures to assist employees with disabilities, while ADA emergency preparedness guidance emphasizes planning for the access and functional needs of people with disabilities. See OSHA's emergency evacuation planning guidance and ADA emergency preparedness resources.