ASIS CPP Exam Questions

Total Questions: 200+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
ASIS CPP Exam Questions by Cert Empire

Question: 1

When handling bullets as evidence, it is most important to avoid:

A. storage at high temperatures.

B. storage at low temperatures.

C. damage to rifling marks on the circumference.

D. damage by dropping them on a hard surface.

Answer:

C

Explanation:

The most critical aspect of a recovered bullet's evidentiary value is the unique microscopic striations (rifling marks) imparted on its surface by the firearm's barrel. These marks are the basis for ballistic forensics, allowing examiners to match the bullet to a specific weapon. Any action that scratches, dents, or otherwise alters these delicate markings can permanently destroy this crucial link. Therefore, the paramount concern in handling a bullet is to preserve the integrity of its circumference where these marks are located.

Why Incorrect Options are Wrong:

A. storage at high temperatures: Normal temperature fluctuations, even high ones, will not alter the metallic structure or the rifling marks on a bullet.
B. storage at low temperatures: Low temperatures have no detrimental effect on the physical characteristics of a solid metal bullet used for forensic comparison.
D. damage by dropping them on a hard surface: While dropping a bullet can cause damage, this is a cause of the problem. The fundamental principle is to avoid damage to the rifling marks (C), which is the ultimate objective.

References:

1. Saferstein, R. (2017). Criminalistics: An Introduction to Forensic Science (12th ed.). Pearson. In Chapter 15, "Firearms, Tool Marks, and Other Impressions," the text emphasizes that "the single most important tool at the firearm examiner's disposal is the comparison microscope," which is used to compare the unique striation markings on bullets. The entire process relies on these marks being pristine (pp. 488-491).
2. ASIS International. (2021). Protection of Assets (POA), Investigations. Section 4.4.3, "Physical Evidence." This section details the fundamental principle of evidence handling, which is to prevent alteration, damage, or contamination. For an item like a bullet, this principle applies most directly to preserving the unique characteristics-the rifling marks-that give it evidentiary value.
3. Federal Bureau of Investigation (FBI). (2019). Handbook of Forensic Services. In the "Evidence

Examinations" section under "Firearms-Toolmarks," the guidelines for submitting evidence implicitly protect these surfaces. For example, it instructs to "Place bullets...in separate containers" and "Do not mark the bullets," which are procedures designed to prevent any damage to the striations on the bullet's surface (p. 28).

Question: 2

Which type of threat is most frequently overlooked and the most difficult to evaluate regarding information assets protection?

A. Inadvertent

B. Natural

C. Cyber

D. Indirect

Answer:

A

Explanation:

Inadvertent threats, which arise from unintentional human error, negligence, or lack of awareness by authorized personnel, are frequently the most overlooked and difficult to evaluate. Security programs often prioritize defending against external, malicious actors (e.g., cyberattacks), underestimating the high frequency and potential impact of internal mistakes. Evaluating this threat is challenging because human behavior is unpredictable, and quantifying the probability of a specific error is nearly impossible with traditional risk assessment models. Unlike natural disasters or defined cyber threats, inadvertent actions lack clear patterns or measurable precursors.

Why Incorrect Options are Wrong:

B. Natural: Natural threats like floods or earthquakes are a fundamental part of business continuity and disaster recovery planning and are rarely overlooked in a comprehensive risk assessment.
C. Cyber: Cyber threats are among the most high-profile and heavily scrutinized risks today; they receive significant attention and resources, making them one of the least overlooked categories.
D. Indirect: Indirect threats, such as utility outages or supply chain disruptions, are a core component of operational risk management and are not typically overlooked in mature security programs.

References:

1. ASIS International. (2021). Protection of Assets: Information Security. Alexandria, VA: ASIS International. In Chapter 2, "Information Security Risk Management," the text emphasizes that human factors are a primary source of risk, stating, "People can be the weakest link in any security program... Threats from insiders can be intentional or unintentional" (p. 2-18). It highlights the difficulty in predicting and mitigating these unintentional actions compared to more structured external threats.

2. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. Chapter 11, "Information Security," discusses the "human element" as a critical vulnerability. The text notes that "unintentional acts or human error... are a major source of computer security problems" and are often more common than malicious attacks, yet harder to predict and control (p. 288).
3. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing (5th ed.). Prentice Hall. Chapter 1, "Is There a Security Problem in Computing?", identifies human errors as a significant and pervasive threat category, noting that "unintentional, non-malicious... human errors are a major source of security vulnerabilities" (p. 29). The text implicitly supports the difficulty in evaluating these unpredictable, non-malicious actions.

Question: 3

Which term describes a limited simulation used to test a business continuity plan?

A. Functional

B. Tabletop

C. Full scale

D. Orientation

Answer:

B

Explanation:

A tabletop exercise is a discussion-based, scenario-driven session where key personnel meet to discuss their roles and responses as outlined in the business continuity plan (BCP). It is considered a "limited simulation" because it tests the plan's logic and the team's understanding of their responsibilities without the physical deployment of resources or personnel. The primary purpose is to identify procedural gaps, clarify roles, and improve decision-making in a low-stress, cost-effective environment. This method effectively validates the planning and coordination aspects of a BCP.

Why Incorrect Options are Wrong:

A. Functional: This is an operations-based exercise that simulates an event in an operational environment to test specific functions, making it more complex than a limited simulation.
C. Full scale: This is the most complex exercise, involving a real-time, multi-agency simulation with actual deployment of resources, far exceeding a "limited" scope.
D. Orientation: This is a low-stress meeting or seminar to familiarize participants with a plan or procedure; it is a form of training, not a test or simulation.

References:

1. ASIS International. (2021). Protection of Assets (POA), Business Continuity. Chapter 5, "Testing, Training, and Exercises." The text distinguishes between discussion-based exercises like tabletops and operations-based exercises like functional and full-scale drills. It describes tabletop exercises as a method to "talk through" a plan to identify weaknesses, which aligns with the concept of a limited simulation.
2. U.S. Department of Homeland Security, Federal Emergency Management Agency (FEMA). (2020). Homeland Security Exercise and Evaluation Program (HSEEP). Section 3, "Exercise Types." This foundational document categorizes exercises as discussion-based or operations-based. It defines a Tabletop Exercise (TTX) as a discussion-based exercise that "involves key personnel discussing simulated scenarios in an informal setting" and is used to

"assess plans, policies, and procedures."

3. George Mason University, Schar School of Policy and Government. (n.d.). EMAP 510: Emergency Exercise Design and Evaluation Course Syllabus. The course materials often reference HSEEP and describe tabletop exercises as a fundamental, discussion-based method for plan validation before progressing to more complex functional or full-scale exercises. This reinforces its role as a limited, foundational simulation.

Question: 4

For access control purposes, it is helpful to divide the high-rise structure into which three classes or types of interior spaces?

A. Lobbies and stairwells, communications and utility points, and mechanical rooms and floors

B. Lower-level, mid-level, and upper-level floors

C. Retail and restaurants, leased or owner-occupied, and public or common areas

D. Public access or common areas, rented or assigned occupancies, and maintenance spaces

Answer:

D

Explanation:

For effective access control management in a high-rise building, security professionals use a zoning approach. This involves classifying interior spaces into three distinct types based on their function and required level of security. These are: 1) Public access or common areas (e.g., lobbies), which have the lowest security restrictions; 2) Rented or assigned occupancies (e.g., tenant offices), which are semi-private and require controlled access; and 3) Maintenance spaces (e.g., mechanical rooms, IT closets), which are restricted areas requiring the highest level of access control due to the critical infrastructure they contain. This classification forms the basis for a layered security strategy.

Why Incorrect Options are Wrong:

A. This option lists specific examples of locations within the three main classes, not the classification system itself.
B. This is a geographical division by floor level, which does not align with the functional security requirements needed for access control zoning.
C. This classification is incomplete because it omits the critical, high-security maintenance and utility spaces that are essential to building operations.

References:

1. ASIS International. (2021). Protection of Assets (POA), Physical Security. Alexandria, VA: ASIS International. In the section on "Special Security Considerations," the text on high-rise buildings outlines the need to divide the interior into zones for access control, identifying these three categories: public areas, tenant areas, and building service/maintenance areas.
2. Garcia, M. L. (2008). The Design and Evaluation of Physical Protection Systems (2nd ed.). Butterworth-Heinemann. Chapter 4, "Facility Characterization," discusses the importance of defining areas by access level (unrestricted, controlled, limited, exclusion) which directly corresponds to the public, tenant, and maintenance space classification.

3. Fennelly, L. J. (Ed.). (2012). Handbook of Loss Prevention and Crime Prevention (5th ed.). Butterworth-Heinemann. Chapter 16, "Physical Security and Crime Prevention," discusses the concept of layered security and zoning, which involves categorizing spaces based on their use and sensitivity, consistent with the public, tenant, and service area model.

Question: 5

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:

The cornerstone of any legally defensible and effective workplace policy, particularly one as sensitive as drug testing, is consistent administration. Consistency ensures fairness, mitigates the risk of discrimination claims, and upholds the integrity of the program. All employees in similar situations must be treated in the same manner according to the established written policy. Arbitrary or inconsistent application can lead to significant legal liability for the organization, including claims of wrongful termination or discrimination based on protected characteristics. The policy's procedures must be uniformly applied to all individuals covered by it.

Why Incorrect Options are Wrong:

A. require mandatory testing of all managers.
This is a specific policy choice, not a universal requirement for all programs, and could be discriminatory if not applied to other employee groups.
B. applied on an "as needed" basis.
This implies arbitrary and inconsistent enforcement, which is a primary basis for legal challenges and undermines the policy's perceived fairness and effectiveness.
C. separate from any collective bargaining agreement.
For unionized workforces, drug testing is typically a mandatory subject of bargaining and must be negotiated and integrated into the collective bargaining agreement (CBA).

References:

1. ASIS International. (2021). Protection of Assets (POA): Personnel. Alexandria, VA: ASIS International. In the chapter on "Substance Abuse in the Workplace," the text emphasizes that a legally defensible drug-testing program must be based on a clear, written policy that is applied consistently and in a non-discriminatory manner to all employees.
2. Fennelly, L. J., & Perry, M. A. (Eds.). (2018). The CPO's Guide to Security Management: A Practical Approach. Butterworth-Heinemann. Chapter 10, "Legal Aspects of Security," discusses that inconsistent application of workplace rules, including drug testing, is a frequent cause of

successful litigation against employers.
3. Kaufman, B. E. (2010). The Development of Human Resource Management Across Nations: Unity and Diversity. Edward Elgar Publishing. In discussions on employee relations and labor law, it is established that for unionized employees, policies affecting terms and conditions of employment, such as drug testing, are mandatory subjects of bargaining under labor laws like the National Labor Relations Act (NLRA) in the United States. This contradicts the notion that such policies should be separate from a CBA. (See discussions on mandatory subjects of bargaining).

Question: 6

A major Crime Prevention Through Environmental Design (CPTED) strategy is to:

A. replace security personnel and security systems.

B. provide clear border definition of controlled spaces.

C. install electronic surveillance equipment compatible with the terrain.

D. eliminate transitional zones between public and private spaces.

Answer:

B

Explanation:

A major strategy of Crime Prevention Through Environmental Design (CPTED) is territorial reinforcement. This principle involves using physical design features to create a clear distinction between public, semi-private, and private spaces. By providing a clear border definition-using elements like fences, landscaping, pavement treatments, and signage-a sense of ownership is established. This signals to potential offenders that they are entering a controlled environment where they are more likely to be challenged, thus deterring criminal activity. This is a foundational concept for creating defensible space.

Why Incorrect Options are Wrong:

A. replace security personnel and security systems.
CPTED is designed to complement and reduce reliance on traditional security measures, not to replace them entirely.
C. install electronic surveillance equipment compatible with the terrain.
CPTED prioritizes natural surveillance (e.g., clear lines of sight) over mechanical or electronic systems, which are considered separate layers of security.
D. eliminate transitional zones between public and private spaces.
CPTED strategically uses and enhances transitional zones to clearly mark the movement from public to private areas, which supports territorial reinforcement.

References:

1. ASIS International. (2021). Protection of Assets: Physical Security. Alexandria, VA: ASIS International. In the chapter on "Crime Prevention Through Environmental Design (CPTED)," the principle of "Territorial Reinforcement" is detailed as the use of physical attributes to express ownership and define spaces, including fences, landscaping, and signage to mark perimeters.
2. Crowe, T. D. (2013). Crime Prevention Through Environmental Design (3rd ed.). Butterworth-Heinemann. Chapter 3, "CPTED Concepts and Strategies," explains that territoriality

is a key strategy that employs real or symbolic barriers (e.g., fences, hedges) to define the boundaries of a space and communicate that it is cared for and controlled.
3. Moffat, R. (1983). Crime Prevention Through Environmental Design-A Management Perspective. Canadian Journal of Criminology, 25(1), 19-31. This academic paper discusses CPTED strategies, emphasizing that "the clear delineation of space" is critical for establishing territoriality and, by extension, defensible space (p. 23). https://doi.org/10.3138/cjcrim.25.1.19

Question: 7

Which method of wiretapping does not require a physical connection to a line?

A. Inductive coupling

B. Connective functioning

C. Active imaging

D. Hardwire connection

Answer:

A

Explanation:

Inductive coupling is a method of electronic eavesdropping that intercepts communications without requiring a direct, physical, or electrical connection to the target wire. It operates by placing a sensor (an induction coil) near the wire, which detects the faint magnetic field that emanates from the wire as electrical signals (representing voice or data) pass through it. This magnetic field induces a corresponding current in the sensor, which is then amplified to reproduce the original communication. This method is passive and non-invasive, making it difficult to detect.

Why Incorrect Options are Wrong:

B. Connective functioning: This is not a recognized technical term for a wiretapping method; it appears to be a distractor option with no standard meaning in this context.
C. Active imaging: This term relates to technologies like radar or sonar that transmit energy and analyze the reflection, which is not a method used for wiretapping telephone lines.
D. Hardwire connection: This method, by definition, requires a direct physical and electrical connection to the communications line (e.g., using alligator clips or splicing wires), which is the opposite of the question's requirement.

References:

1. ASIS International. (2021). Protection of Assets (POA), Information Security. Chapter 5: Technical Surveillance and Countermeasures. This chapter details various eavesdropping techniques, describing inductive taps (or induction coil taps) as a primary method for non-contact interception of signals from wiring by detecting electromagnetic emanations.
2. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In Chapter 14, "Information Security," the text discusses electronic eavesdropping methods, explaining that inductive taps do not require the wire's insulation to be stripped, as they work by picking up the magnetic flux surrounding the conductor.
3. Broder, J. F. (2012). Risk Analysis and the Security Survey (4th ed.). Butterworth-Heinemann. Chapter 11, "The Security Survey," discusses technical security and surveillance, identifying

inductive wiretaps as a common, non-invasive threat that TSCM (Technical Surveillance Countermeasures) teams screen for.

Question: 8

The three types of line transmissions in electronic protection systems are:

A. loop, Doppler. and multiplex.

B. point-to-point, Doppler, and multiplex.

C. Doppler, point-to-point, and loop.

D. loop, point-to-point, and multiplex.

Answer:

D

Explanation:

The question asks to identify the methods of line transmission, which refers to how alarm signals are communicated from sensors to a control panel. The three primary types are loop, point-to-point, and multiplex.
Loop: A simple circuit where sensors are wired in series or parallel. An alarm is triggered by a change in the circuit's electrical state (e.g., an open or short).
Point-to-point: Each sensor or a small group of sensors (a zone) has a dedicated, direct wiring connection to the control panel.

Multiplex: An advanced method where signals from multiple, individually addressable sensors are combined and transmitted over a single communication line or data bus.

Why Incorrect Options are Wrong:

A. Incorrect. Doppler is a principle of sensor operation (e.g., microwave motion detectors), not a method of line transmission.
B. Incorrect. Doppler is a sensor technology used for motion detection, not a type of signal wiring or transmission.
C. Incorrect. Doppler describes how a specific type of sensor functions, not how its signal is transmitted to a control panel.

References:

1. ASIS International. (2021). Protection of Assets (POA), Physical Security. Alexandria, VA: ASIS International. In the chapter on "Intrusion Detection and Assessment Systems," the text distinguishes between sensor technologies and signal transmission methods. It details loop circuits, point-to-point (or zoned) wiring, and multiplex/addressable systems as the primary means of alarm signal transmission (Section 4.5.3, "Alarm Signal Transmission").
2. Garcia, M. L. (2007). The Design and Evaluation of Physical Protection Systems (2nd ed.). Butterworth-Heinemann. Chapter 6, "Intrusion Detection Systems," discusses alarm communication and data transmission, describing multiplexing as a method to reduce wiring

complexity by sending multiple sensor signals over a common line, and contrasts it with simpler direct-wire (point-to-point) and loop circuits (pp. 135-137).
3. Fennelly, L. J. (2012). Effective Physical Security (4th ed.). Butterworth-Heinemann. Chapter 15, "Alarm Systems," explains the evolution of alarm wiring from basic loops to zoned (point-to-point) systems and modern addressable multiplex systems that provide specific point identification (pp. 289-291). The Doppler effect is discussed separately as a motion detection technology.

Question: 9

Which method of wiretapping does not require a physical connection to a line?

A. Inductive coupling

B. Connective junctioning

C. Active imaging

D. Hardwire connection

Answer:

A

Explanation:

Inductive coupling is a method of signal interception that does not require direct physical or electrical contact with the target wire. This technique utilizes an induction coil placed in close proximity to the wire. The electrical current flowing through the wire generates a fluctuating electromagnetic field around it. This field, in turn, induces a small, corresponding electrical current in the nearby coil. The induced signal is then amplified to reconstruct the original communication (e.g., voice or data). Because it only requires proximity to the wire's magnetic field, it is considered a non-invasive or "contactless" form of wiretapping.

Why Incorrect Options are Wrong:

B. Connective junctioning: This is not a standard technical term; however, the word "connective" implies a physical link, which is contrary to the question's requirement.
C. Active imaging: This term is associated with technologies like radar or thermal imaging that create visual representations and is not a method for intercepting electrical signals from a wire.
D. Hardwire connection: This is a direct physical tap where the eavesdropping device is electrically connected to the target line, which is the opposite of the method sought.

References:

1. Fennelly, L. J., & Perry, M. A. (Eds.). (2018). The Criminology of Security. In Protection of Assets. ASIS International. In the section discussing Technical Surveillance Countermeasures (TSCM), the principles of signal emanation are detailed, explaining how inductive devices can capture signals without physical connection by detecting the magnetic flux field around a conductor.
2. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. Chapter 13, "Information Security," describes various methods of electronic eavesdropping, distinguishing between direct "hardwire" taps and indirect methods like inductive coupling that intercept radiated signals.
3. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing (5th ed.). Prentice

Hall. Chapter 9, "Privacy," discusses threats to communication privacy, including wiretapping. The text explains the physics behind signal interception, where inductive taps exploit the electromagnetic emanations from current-carrying wires, a principle of non-contact interception.

Question: 10

The three types of line transmissions in electronic protection systems are:

A. loop, Doppler. and multiplex.

B. point-to-point. Doppler, and multiplex.

C. Doppler, point-to-point, and loop.

D. loop, point-to-point, and multiplex.

Answer:

D

Explanation:

In electronic protection systems, line transmission refers to the method by which signals from sensors are sent to a control panel. The three primary types are:
1. Loop: A simple series circuit where multiple sensors are wired together. An alarm is triggered if the circuit's electrical continuity is broken or shorted.
2. Point-to-point: Each sensor has its own dedicated wire pair running directly to the control panel, allowing for individual sensor identification.
3. Multiplex: A more advanced method where signals from multiple sensors are encoded and transmitted over a single communication line, with each sensor having a unique address.

Why Incorrect Options are Wrong:

A. This option is incorrect because Doppler is a principle of motion detection technology (e.g., in microwave sensors), not a type of line transmission.
B. This option is incorrect because it includes Doppler, which is a sensing technology used to detect motion, not a method for transmitting alarm signals.
C. This option is incorrect as it also includes Doppler, a motion sensing principle, rather than a method of signal transmission over a line.

References:

1. Fischer, R. J., Halibozek, E. P., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In Chapter 11, "Physical Security II: The Application," the text describes alarm system wiring, detailing series circuits (loops), direct wire (point-to-point), and multiplexing as methods for connecting sensors to control panels (pp. 268-269).
2. ASIS International. (2021). Protection of Assets (POA), Physical Security. In the chapter "Intrusion Detection Systems," Section 3.3, "Signal Transmission," the text outlines the evolution and types of alarm circuits, including simple loops, point-to-point (addressable) systems, and multiplexed systems which transmit data from multiple sensors over a shared line.
3. Garcia, M. L. (2007). The Design and Evaluation of Physical Protection Systems (2nd ed.).

Butterworth-Heinemann. Chapter 6, "Intrusion Detection," discusses alarm communication and data transmission, differentiating between sensor technologies (like Doppler microwave) and the communication paths (such as hardwired loops, point-to-point, and multiplexed data lines) that carry signals to an annunciator (pp. 135-138).

Question: 11

A financial decision tool that measures the productivity of assets by computing profits as a percentage of capital invested is known as a/an:

A. marginal analysis.

B. investment forecast

C. return on investment

D. breakeven analysis

Answer:

C

Explanation:

Return on Investment (ROI) is a financial performance metric used to evaluate the efficiency and profitability of an investment. It is calculated by dividing the net profit (or return) from an investment by the cost of the investment. The result is expressed as a percentage or a ratio and directly measures the productivity of the capital invested, which precisely matches the definition provided in the question. It is a fundamental tool for making financial decisions and justifying security expenditures by demonstrating their value.

Why Incorrect Options are Wrong:

A. Marginal analysis: This tool examines the costs and benefits of incremental changes, such as producing one more unit, not the overall productivity of an entire investment.
B. Investment forecast: This is a prediction or estimation of an investment's future performance, not a calculation of its actual, realized productivity based on profits.
D. Breakeven analysis: This determines the point at which total costs and total revenue are equal, indicating no net loss or gain, rather than measuring profitability as a percentage.

References:

1. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In the context of security program justification, the text discusses financial metrics, stating, "Return on investment (ROI) is a profitability ratio that measures the gain or loss from an investment relative to its cost." (Chapter 5, Security and the Business, Financial Management section).
2. ASIS International. (2021). Protection of Assets (POA), Business Principles. In the section on Financial Controls, ROI is defined as a key performance indicator for evaluating the financial consequences of an investment. It is presented as (Gain from Investment - Cost of Investment) / Cost of Investment, which is the standard formula for calculating profit as a percentage of capital. (Section 3.4.2, Justifying Security Program Expenditures).

3. Parrino, R., Kidwell, D. S., & Bates, T. W. (2012). Fundamentals of Corporate Finance (2nd ed.). John Wiley & Sons. University-level finance texts define ROI as a measure of the efficiency with which assets are used to generate profits. "Return on investment (ROI) measures the income generated by the assets of the firm." (Chapter 3, Financial Analysis and Planning, p. 76).

Question: 12

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 (PIR) sensors are specifically designed to detect the infrared energy (heat) that is naturally radiated by the human body. These sensors are passive, meaning they do not emit energy. Instead, they measure the differential in infrared radiation between a moving person and the background environment. When a person enters the sensor's field of view, the change in thermal energy is detected, which in turn triggers an alarm. This makes them a common and effective technology for intrusion detection based on body heat.

Why Incorrect Options are Wrong:

A. Microwave: This is an active sensor that detects motion by transmitting microwave signals and analyzing the frequency shift of the reflected signals, not by sensing heat.
C. Temperature: This type of sensor measures ambient temperature for environmental control or fire detection, not the specific infrared signature of a moving person for intrusion.
D. Ultrasonic: This is an active sensor that detects motion by emitting high-frequency sound waves and detecting changes in the reflected sound patterns.

References:

1. ASIS International. (2021). Protection of Assets: Physical Security. Alexandria, VA: ASIS International. In the chapter on "Intrusion Detection Systems," the section on "Interior Sensors" states, "Passive infrared (PIR) sensors detect thermal energy (heat) in the form of infrared radiation... The human body is a prime source of infrared radiation."
2. Garcia, M. L. (2008). The Design and Evaluation of Physical Protection Systems (2nd ed.). Butterworth-Heinemann. In Chapter 5, "Sensors," it is explained that "Passive infrared (PIR) sensors detect the thermal energy emitted by an intruder... The sensor detects a change in the thermal energy of its field of view and initiates an alarm" (p. 103).
3. Fennelly, L. J., & Perry, M. A. (Eds.). (2021). The Criminology of Physical Security: A Global Perspective. CRC Press. Chapter 10, "Intrusion Detection Systems," describes PIR detectors: "These devices are passive, meaning they do not transmit a signal but rather receive the infrared

energy (heat) from an intruder."

Question: 13

A business impact analysis provides management information on:

A. resources that are available on site, who is working in critical positions, the cost of the facility, and
testing of the plan of action.

B. what can happen, what will be affected, and resources that will be needed to reestablish business
functions

C. organized responder notification, incident command structure, testing of the plan of action, and the cost of the facility.

D. responsibilities of management personnel, the levels of disasters and emergencies, media response techniques, and shelter areas.

Answer:

B

Explanation:

A Business Impact Analysis (BIA) is a foundational process in business continuity management.

Its primary purpose is to identify an organization's critical business functions and processes and to determine the potential impacts resulting from a disruption to them. The BIA process analyzes various disruption scenarios ("what can happen"), identifies the specific functions and dependent resources that would be affected ("what will be affected"), and quantifies the resources required to resume those functions within a predetermined timeframe ("resources that will be needed to reestablish business functions"). This information is crucial for management to make informed decisions about risk mitigation and resource allocation for continuity planning.

Why Incorrect Options are Wrong:

A. This option incorrectly includes "testing of the plan of action," which occurs after the BIA and plan development, and "cost of the facility," which is a general operating expense, not a BIA focus.
C. This option lists elements of an emergency response or incident management plan (responder notification, incident command structure), not the analytical outputs of a BIA.
D. This option describes components of crisis management and emergency response plans (management responsibilities, media response, shelter areas), which are distinct from a BIA.

References:

1. ASIS International. (2021). Protection of Assets (POA). In the volume on Crisis Management, the chapter on Business Continuity Management specifies that the BIA is the process used to identify critical business processes, the impact of a disruption, and the resources required for recovery. It serves as the foundation for strategy development.
2. National Institute of Standards and Technology (NIST). (2010). Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. Section 3.2, "Business Impact Analysis," states, "The BIA process analyzes the business processes and the effect that a specific disaster may have on them... The BIA should identify the resources that are required for the business process to be recovered."
3. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements. Clause 8.2.2, "Business impact analysis," requires the organization to "identify the processes that support the delivery of its products and services," "assess the impacts over time of not resuming these processes," and "identify the resources needed by processes."

Question: 14

In large-scale emergencies, the Incident Command System can be effectively deployed by:

A. private sector organizations only.

B. federal agencies only.

C. public and private sector organizations.

D. public sector organizations only.

Answer:

C

Explanation:

The Incident Command System (ICS) is a standardized, on-scene, all-hazards incident management approach. It is a fundamental component of the National Incident Management System (NIMS). NIMS is designed to provide a common operating framework for all organizations involved in emergency response, including governmental agencies at all levels (federal, state, local, tribal), non-governmental organizations (NGOs), and private sector entities. This integration is critical during large-scale emergencies, where a coordinated effort between public first responders and private sector resources (e.g., critical infrastructure, businesses) is essential for an effective response and recovery. Therefore, ICS can and should be deployed by both public and private organizations.

Why Incorrect Options are Wrong:

A. private sector organizations only: This is incorrect because ICS was developed within the public sector and is a standard for government emergency response agencies.
B. federal agencies only: This is incorrect as ICS is designed for use by all levels of government, including state, local, and tribal, not just federal entities.
D. public sector organizations only: This is incorrect because NIMS explicitly includes the private sector as a key partner, and its adoption of ICS is crucial for interoperability.

References:

1. Federal Emergency Management Agency (FEMA). (2017). National Incident Management System (NIMS), Third Edition. U.S. Department of Homeland Security. On page 2, under "Applicability and Scope," it states, "NIMS is applicable to all stakeholders with roles in incident management... This includes all levels of government (Federal, State, local, tribal, and territorial), nongovernmental organizations (NGO), and the private sector."
2. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In Chapter 14, "Emergency Management and Homeland Security," the text discusses the importance of public-private partnerships and the adoption of NIMS and ICS by

the private sector to ensure effective, integrated response to emergencies.

3. ASIS International. (2021). Protection of Assets (POA) Manual. The volume on Crisis Management details the structure and application of the Incident Command System, emphasizing its role in coordinating efforts between public and private entities during a crisis. It highlights that security professionals must be proficient in ICS to effectively interface with first responders.

Question: 15

Which of the following represents the crossover error rate for biometric technology?

A. It measures the acceptable number of failures that a security firm is willing to tolerate.

B. The point at which the number of false rejections equals the false acceptances.

C. The frequency of false rejections.

D. The point at which the number of positive rejections equals the false acceptances.

Answer:

B

Explanation:

The Crossover Error Rate (CER), also known as the Equal Error Rate (EER), is a standard metric used to measure the overall accuracy of a biometric system. It represents the specific point on a system's sensitivity scale where the False Acceptance Rate (FAR) is equal to the False Rejection Rate (FRR). A lower CER value indicates a more accurate and reliable system, as it signifies a lower number of both false acceptances and false rejections at its optimal setting. This single-figure metric is crucial for comparing the performance of different biometric devices.

Why Incorrect Options are Wrong:

A. This describes a security organization's risk tolerance or acceptable risk level, which is a business decision, not a specific performance metric of a biometric system.
C. This defines only the False Rejection Rate (FRR) or Type I error, which is the probability that the system incorrectly rejects a valid, authorized user.
D. The term "positive rejections" is not standard terminology in biometrics. The correct terms are False Rejection Rate (FRR) and False Acceptance Rate (FAR).

References:

1. Fennelly, L. J., & Perry, M. A. (Eds.). (2021). The Professional Protection Officer: Practical Security Strategies and Emerging Trends (2nd ed.). Butterworth-Heinemann. In the chapter on Access Control, it is explained that the Crossover Error Rate (CER) is the point where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are equal, serving as a key indicator of a biometric system's accuracy. (Chapter 11, Access Control Systems).
2. Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer. "The Equal Error Rate or EER is the point on a ROC (or DET) curve where the FAR equals the FRR. A lower EER value indicates better performance." (Chapter 1, Section 1.5.2, p. 23).
3. ASIS International. (2012). Protection of Assets (POA), Physical Security. "The crossover error rate (CER) is the point at which the percentage of false acceptances is equal to the percentage of false rejections. The CER is often used to gauge the overall accuracy of a biometric system."

(Physical Security volume, Section on Biometric Access Control Systems).

Question: 16

In large-scale emergencies, the Incident Command System can be effectively deployed by:

A. private sector organizations only.

B. federal agencies only.

C. public and private sector organizations.

D. public sector organizations only.

Answer:

C

Explanation:

The Incident Command System (ICS) is a core component of the U.S. National Incident Management System (NIMS). NIMS establishes a standardized, all-hazards approach to incident management, designed to be used by all levels of government (federal, state, local, tribal), nongovernmental organizations, and the private sector. This "whole community" approach is essential for effective management of large-scale emergencies, as it enables seamless integration and interoperability between different entities. The scalability and flexibility of ICS allow it to be adopted by any organization to manage incidents and to coordinate effectively with external response partners.

Why Incorrect Options are Wrong:

A. ICS is not limited to the private sector; it originated in the public sector and is a standard for government response.
B. ICS is used by all levels of government (local, state, tribal, and federal), not exclusively by federal agencies.
D. The private sector is a critical partner in emergency management and is strongly encouraged by NIMS to adopt and use ICS.

References:

1. Federal Emergency Management Agency (FEMA). (2017). National Incident Management System (NIMS) Doctrine. FEMA P-1000.
Page 1, Introduction: "NIMS provides a common, nationwide approach that enables the whole community to work together to manage all threats and hazards. NIMS is applicable to all stakeholders with incident management and support responsibilities... This includes all levels of government, nongovernmental organizations (NGOs), and the private sector."
Page 4, Scope: "NIMS is applicable to all incidents... It is a comprehensive framework that can be used by all stakeholders... including governmental entities at all levels, NGOs, and the private sector."

2. ASIS International. (2021). Protection of Assets (POA), Crisis Management.
Chapter 3, Incident Management, Section on National Incident Management System (NIMS): This section details that NIMS provides a consistent framework for government, the private sector, and nongovernmental organizations to collaborate. It emphasizes that private sector organizations should adopt ICS to effectively interface with public sector first responders during an incident.
3. Jensen, J. L. (2010). Business's Role in Emergency Preparedness and Response: A Guide to Inter-organizational, Public-Private Collaboration. Naval Postgraduate School.
Page 11, Section on NIMS: "NIMS provides a consistent nationwide template to enable Federal, State, local, and tribal governments, the private sector, and nongovernmental organizations to work together to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity."

Question: 17

Which of the following represents the crossover error rate for biometric technology?

A. It measures the acceptable number of failures that a security firm is willing to tolerate.

B. The point at which the number of false rejections equals the false acceptances.

C. The frequency of false rejections.

D. The point at which the number of positive rejections equals the false acceptances.

Answer:

B

Explanation:

The Crossover Error Rate (CER), also known as the Equal Error Rate (EER), is a standard metric used to measure the overall accuracy of a biometric system. It is the point at which the system's sensitivity is set so that the False Acceptance Rate (FAR) is equal to the False Rejection Rate (FRR). A lower CER indicates a more accurate system, as it represents the point where both types of errors are minimized simultaneously. This single value provides a way to compare the performance of different biometric systems under their optimal operational threshold.

Why Incorrect Options are Wrong:

A. This describes a business decision related to risk tolerance or an acceptable quality level, not the specific technical performance metric of CER.
C. This describes only the False Rejection Rate (FRR), which is the probability that an authorized user is incorrectly denied access.
D. The term "positive rejections" is not standard biometric terminology. The CER is where the False Rejection Rate equals the False Acceptance Rate.

References:

1. Fennelly, L. J., & Perry, M. A. (Eds.). (2021). The Professional Protection Officer: Practical Security Strategies and Emerging Trends (2nd ed.). ASIS International & Butterworth-Heinemann. In discussions of biometric access control, the text defines the Equal Error Rate (EER) or Crossover Error Rate (CER) as the point where the false-accept rate and false-reject rate are equal (Chapter 11, Access Control Systems).
2. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20. Section III-C, "Performance," states: "The performance of a biometric system is often measured in terms of the false accept rate (FAR) and the false reject rate (FRR)... The EER is the point where the FAR and FRR are equal." (p. 10). DOI: https://doi.org/10.1109/TCSVT.2003.818349
3. ASIS International. (2012). Protection of Assets (POA), Physical Security. The section on

"Biometric Access Control" describes performance metrics, including the Crossover Error Rate (CER) as the point where the probability of a false acceptance is the same as the probability of a false rejection.

Question: 18

The purpose of applicant screening is to:

A. limit the liability exposure if the hired person assaults co-workers or customers.

B. find the most appropriate person for a particular job.

C. reduce reliance on interviewing and testing.

D. make a choice with the minimum possible investment of personnel, money, and time.

Answer:

B

Explanation:

The fundamental purpose of the applicant screening process is to identify the most suitable and qualified candidate for a specific job. Screening is the initial step in the overall selection process, where an applicant's qualifications, experience, and other attributes are compared against the job requirements. This filtering mechanism ensures that only those who meet the minimum criteria proceed to more in-depth evaluation stages like interviews and testing. The ultimate goal is to achieve the best possible match between the person, the position, and the organization, thereby maximizing the potential for job success and employee retention.

Why Incorrect Options are Wrong:

A. Limiting liability exposure, such as for negligent hiring, is a critical secondary benefit and a risk management outcome of screening, not its primary purpose.
C. Screening is a preliminary step that complements and makes subsequent stages like interviewing and testing more efficient; it does not reduce reliance on them.
D. While efficiency is desirable, the primary objective is to find the most effective and appropriate candidate, not simply to minimize the cost or time of hiring.

References:

1. ASIS International. (2021). Protection of Assets (POA): Personnel Protection. Alexandria, VA: ASIS International. Chapter 2, "Preemployment Measures," Section 2.2, "The Selection Process." The text explains that the goal of the selection process, which begins with screening, is to hire the best-qualified individual by matching their knowledge, skills, and abilities to the job requirements.
2. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. Chapter 11, "Personnel Security," discusses preemployment screening as a key function to ensure the suitability, reliability, and integrity of candidates, which directly supports the objective of finding the most appropriate person for the job.
3. ASIS International. (2019). Preemployment Background Screening Guideline (ASIS GDL PBS-2019). Alexandria, VA: ASIS International. Section 4, "Guideline Elements," outlines the

purpose of screening as a due diligence process to verify candidate information and assess suitability for employment, which is integral to selecting the most appropriate person.

Question: 19

Choosing a security container for a specific software application is largely determined by value and what other characteristic of the item to be stored?

A. Vulnerability

B. Commonality

C. Place of origin

D. Reproducibility

Answer:

A

Explanation:

The selection of appropriate security measures, such as a security container, is a fundamental outcome of the risk assessment process. Risk is commonly defined as a function of an asset's value, the threats against it, and its vulnerabilities. The question already provides "value" as one determinant. The other critical characteristic is "vulnerability," which is any weakness that can be exploited by a threat to cause harm to the asset. Therefore, a highly valuable asset that is also highly vulnerable requires the most stringent protective measures.

Why Incorrect Options are Wrong:

B. Commonality: The commonality of an item may relate to its replaceability or value, but it is not a direct factor in the risk formula used to determine protection levels.
C. Place of origin: An item's origin is generally not a primary consideration for selecting a security container, unless it pertains to specific geopolitical threats or regulatory controls.
D. Reproducibility: While reproducibility affects recovery planning and overall business impact, vulnerability is the direct characteristic that a security measure is designed to mitigate to prevent loss in the first place.

References:

1. ASIS International. (2021). Protection of Assets: Security Management. Alexandria, VA: ASIS International. The chapter on "Risk Management" explains that risk analysis involves identifying assets, their value, and their vulnerabilities to specific threats. The selection of countermeasures is based on mitigating these identified vulnerabilities.
2. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In Chapter 5, "The Security Risk Assessment," the text emphasizes that a vulnerability assessment is a critical step. It states, "A vulnerability is a weakness... The purpose of the security survey is to identify these vulnerabilities so that countermeasures can be implemented" (p. 104).

3. Garcia, M. L. (2008). The Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann. Chapter 2, "Systematic Approach to Physical Protection System Design," outlines that the characterization of a facility or asset includes identifying vulnerabilities. The design of the protection system (e.g., containers, barriers) is a direct response to these vulnerabilities in relation to defined threats.

Question: 20

An organization's Chief Executive Officer (CEO) wants to expand surveillance technology at their main distribution center as part of an employee theft and misconduct reduction initiative. Which of the following should the security management team advise the CEO of regarding privacy considerations?

A. The additional cameras should be hidden so that employees do not know that they are under surveillance.

B. The CEO should invest in other types of technology to deter crime and misconduct due to privacy
considerations

C. The new surveillance system should utilize IP cameras that are capable of recording audio as well
as video.

D. Consult with HR and legal to ensure no cameras are recording in areas where employees have a
reasonable expectation of privacy.

Answer:

D

Explanation:

The paramount consideration in implementing workplace surveillance is the employee's "reasonable expectation of privacy," a legal standard that protects individuals in specific areas. Placing surveillance devices in locations such as restrooms, locker rooms, or break areas can lead to significant legal and civil liabilities. The most prudent and professional course of action is to engage legal counsel and Human Resources (HR). This ensures the surveillance program is designed and implemented in full compliance with federal, state, and local laws (e.g., wiretapping statutes, NLRB guidance), as well as internal corporate policies. This collaborative approach effectively balances the organization's legitimate security interests with its legal and ethical obligations to its employees.

Why Incorrect Options are Wrong:

A. Covert surveillance of employees is highly regulated, often illegal without specific cause, and can severely damage employee morale and trust.
B. This option prematurely dismisses a valid security tool instead of exploring how to implement it in a legally compliant and ethical manner.
C. Recording audio without the consent of all parties is illegal in many jurisdictions under wiretapping laws and dramatically increases the organization's legal risk.

References:

1. ASIS International. (2021). Protection of Assets (POA), Legal Aspects. Alexandria, VA: ASIS International. The text emphasizes that "the most significant legal issue in the use of CCTV is privacy" and strongly advises security professionals to seek legal counsel to navigate the complex web of federal and state laws. It specifically discusses the "reasonable expectation of privacy" standard for areas like locker rooms and restrooms. (Section on "Information Security and Privacy").
2. ASIS International. (2021). Protection of Assets (POA), Physical Security. Alexandria, VA: ASIS International. This volume details the implementation of video surveillance systems and notes that a "video surveillance policy should be developed in consultation with the legal department and human resources" to address privacy and other legal considerations before installation. (Chapter on "Video Surveillance").
3. Fennelly, L. J. (2017). Effective Physical Security (5th ed.). Butterworth-Heinemann. As a foundational text in the security field, it states that legal counsel must be consulted on surveillance activities, particularly regarding audio recording, which is generally prohibited, and camera placement to avoid infringing on privacy rights in sensitive areas. (Chapter 25: CCTV Technology).
4. Cornell University Law School, Legal Information Institute (LII). "The Fourth Amendment's protection against unreasonable searches and seizures by the government has been interpreted to provide a basis for a right to privacy... This concept is often discussed in terms of a 'reasonable expectation of privacy'." While focused on government action, this principle is the foundation for privacy law that extends into private-sector employment law. (Article on "Privacy").

Question: 21

The role of supervisors in the enforcement of a company's substance abuse policy is to:

A. detect employee drug use.

B. monitor employee performance.

C. identity employees selling drugs.

D. refer employees for counseling services.

Answer:

D

Explanation:

Within a drug-free-workplace programme supervisors are trained to deal only with job-related problems they can legitimately address. Their task is to document impaired performance and initiate a formal "supervisory referral" to the organisation's Employee Assistance Program or other counselling resource. Diagnosing drug use or investigating trafficking is outside their competence, and merely "monitoring performance" is a normal managerial duty, not the specific enforcement step required by the substance-abuse policy.

Why Incorrect Options are Wrong:

A. Detecting drug use is a medical/testing function; supervisors are not qualified and risk legal liability if they attempt diagnosis.
B. Performance monitoring is routine management; enforcement requires the next step-referral to professional help when abuse is suspected.
C. Identifying on-site drug sales involves security or law-enforcement investigators, not line supervisors.

References:

1. ASIS International, Protection of Assets Manual, Vol. 2 "Security Management", Section "Substance-Abuse Programs", pp. 2-35-2-36: supervisors document performance problems and make EAP referrals.
2. Roman, P.M. & Blum, T.C. (1996) "The workplace and alcohol problem prevention", Alcohol Health & Research World 20(4), p. 252 2: supervisors refer employees to counselling/EAP; they do not diagnose. DOI:10.1037/e494522006-002
3. MIT OpenCourseWare, Course 15.668 People and Organizations, Session 12 "Employee Assistance Programs", Slide 6: supervisor's key role-formal referral to counselling resources when performance deteriorates.
4. Journal of Occupational & Environmental Medicine, 37(7) (1995) "Supervisor training and EAP referral patterns", pp. 784-785: performance documentation followed by supervisory referral is the

mandated process.

5. University of Washington School of Public Health, Workplace Substance-Abuse Module, Section "Supervisor Responsibilities", para 3: supervisors observe, document, and refer to EAP-not detect use or investigate sales.

Question: 22

While the scope of training for an emergency depends on the nature of the organization's activities, this training must:

A. be given to all employees, visitors, and contractors.

B. cover all aspects of the emergency plan for all participants.

C. be reinforced and tested with periodic drills.

D. be reinforced and tested on a quarterly basis.

Answer:

C

Explanation:

The effectiveness of any emergency training program is contingent upon its regular reinforcement and validation. Periodic drills and exercises are fundamental components of a robust emergency management system. They serve to test the viability of the plan, ensure personnel are familiar with their roles and responsibilities, identify procedural gaps, and build the "muscle memory" necessary for an effective response under stress. This cycle of training, testing, and refinement is a universally accepted best practice for ensuring organizational preparedness, regardless of the specific nature of the emergency.

Why Incorrect Options are Wrong:

A. be given to all employees, visitors, and contractors. Training should be role-specific and appropriate to the audience; visitors and contractors typically receive a briefing, not the same in-depth training as employees.
B. cover all aspects of the emergency plan for all participants. Information is provided on a need-to-know basis; most personnel only need training on their specific roles, not the entire comprehensive plan.
D. be reinforced and tested on a quarterly basis. The frequency of drills is determined by risk analysis, regulatory requirements, and organizational complexity; a fixed quarterly schedule is overly prescriptive and not a universal rule.

References:

1. ASIS International. (2021). Protection of Assets (POA), Crisis Management. Section 3.5.3, "Training, Drills, and Exercises." This section emphasizes that plans must be validated and personnel skills maintained through a program of drills and exercises, stating, "A crisis management plan that is not tested is of little value... Drills and exercises are the primary tools for testing the plan."
2. Federal Emergency Management Agency (FEMA). (2020). Homeland Security Exercise and

Evaluation Program (HSEEP). Chapter 2, "Exercise Program Management." The doctrine establishes that exercises are "the primary tool for assessing preparedness and identifying gaps" and are essential for "validating plans and procedures, and training and familiarizing personnel."
3. Borodzicz, E. P. (2005). Risk, Crisis and Security Management. John Wiley & Sons. Chapter 8, "Training and Exercising." The text explains that training and exercising are critical for developing competence and confidence in emergency response. It states that exercises are necessary to "test the viability of plans" and "reinforce training" to ensure procedures are workable in a real event.

Question: 23

In terms of information systems security (ISS), "residual risk" is:

A. the total remaining potential risk after all ISS countermeasures are applied across all threats.

B. the remaining potential risk for each threat after all ISS countermeasures are applied.

C. the product of the level of threat and the level of vulnerability

D. equal to threats multiplied by countermeasures and divided by vulnerabilities.

Answer:

B

Explanation:

Residual risk is a core concept in risk management, defined as the risk that remains after security controls and countermeasures have been implemented. The risk management process involves identifying specific threats, assessing their likelihood and potential impact, and then applying controls to mitigate them. Residual risk is the calculated, remaining risk exposure for each specific threat that has been treated, which management must then decide to accept, transfer, or mitigate further.

Why Incorrect Options are Wrong:

A. This describes the total or aggregate residual risk profile of an organization, not the fundamental definition. Residual risk is first calculated on a per-threat basis.
C. This is the basic formula for calculating inherent risk or initial risk (Risk = Threat x Vulnerability), not the risk remaining after controls are applied.
D. This is an illogical and incorrect formula. Countermeasures are designed to reduce risk, not act as a multiplier in a risk calculation.

References:

1. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In Chapter 5, "The Role of Risk Analysis in Security," the concept is explained as the risk that "remains after countermeasures have been implemented." The process described involves analyzing individual risks, applying countermeasures, and then determining the leftover or residual risk for those specific items.
2. National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (NIST Special Publication 800-30, Revision 1). In Appendix F, Glossary, "Residual Risk" is defined as the "Portion of risk remaining after security controls have been applied." The entire methodology of the guide is based on assessing risk from specific threat events (Section 2.2.2) and then determining the residual risk for those events after controls are considered (Section 2.4).

3. ASIS International. (2012). Protection of Assets (POA). Alexandria, VA: ASIS International. The Security Management volume details the risk management process. It specifies that after risk analysis and the application of countermeasures, a residual risk remains. This evaluation is performed for the specific risks identified during the assessment to determine if they are at an acceptable level for the organization.

Question: 24

Which of the following types of intrusion detection systems is commonly used to protect safes and file cabinets?

A. Pin core

B. Pick resistant

C. Capacitance

D. Electro-mechanical

Answer:

C

Explanation:

Capacitance proximity sensors are a type of intrusion detection system specifically designed to protect conductive objects like metal safes and file cabinets. The system works by creating a stable electrostatic field around the protected object. When a person, who is also conductive, approaches or touches the object, their body adds capacitance to the circuit. This change disrupts the electrostatic field, which is detected by the sensor's control unit, triggering an alarm. This method provides excellent protection for specific, high-value assets by detecting an intruder's presence before they can breach the container.

Why Incorrect Options are Wrong:

A. Pin core: This refers to a component of a mechanical lock cylinder, not an electronic intrusion detection system.
B. Pick resistant: This is a characteristic describing a mechanical lock's ability to withstand covert manipulation, not a type of sensor.
D. Electro-mechanical: This is a broad classification of devices. While a safe might use an electro-mechanical bolt switch, a capacitance sensor is the specific technology used for proximity detection.

References:

1. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In Chapter 11, "Physical Security I: The Role of Barriers, Alarms, and Lighting," the text describes interior intrusion sensors, noting that capacitance proximity detectors are used to protect specific objects like safes and filing cabinets by sensing a change in the electrical field when a person approaches. (See section on "Proximity or Capacitance Detectors").
2. Garcia, M. L. (2007). The Design and Evaluation of Physical Protection Systems (2nd ed.). Butterworth-Heinemann. Chapter 5, "Detection and Assessment," discusses interior sensors. It explains that proximity sensors, including capacitance types, are used to detect an intruder

touching or coming near a specific asset, with safes and vaults being primary examples of their application (pp. 89-90).
3. ASIS International. (2016). Protection of Assets (POA), Physical Security. In the volume on Physical Security, the section covering Interior Intrusion Detection Systems details the function of capacitance proximity detectors. It explicitly states their common application is for the protection of metal objects, including safes, vaults, and file cabinets, by detecting the change in capacitance caused by a human body.

Question: 25

Which factor about a risk would make it uninsurable?

A. Losses would be expected but unintended by the insured.

B. Losses could not be positively tied to an occurrence in an established amount.

C. The risk is predictable through the law of large numbers.

D. The risk would be worth the cost but not the effort to insure.

Answer:

B

Explanation:

For a risk to be insurable, the potential loss must be definite and measurable. This means the insurer must be able to determine when a loss has occurred (a specific occurrence) and be able to calculate the financial value of that loss (an established amount). If a loss cannot be clearly linked to a specific event or its value cannot be quantified, the insurer cannot determine a fair premium or the appropriate indemnity to pay. This lack of definiteness and measurability makes the risk fundamentally uninsurable.

Why Incorrect Options are Wrong:

A. Losses would be expected but unintended by the insured.
This describes an insurable risk. Losses must be unintended (fortuitous), and insurers use statistics to expect losses across a large pool of insureds.
C. The risk is predictable through the law of large numbers.
This is a core principle that makes a risk insurable, not uninsurable. It allows insurers to forecast losses and set appropriate premiums.
D. The risk would be worth the cost but not the effort to insure.
This reflects a subjective business decision by the potential insured, not an inherent characteristic that makes the risk uninsurable from an insurer's perspective.

References:

1. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In the discussion of risk transfer, the text outlines the requirements for an insurable risk, emphasizing that a loss must be measurable and definite in time, place, and amount. A failure to meet this criterion, as described in option B, renders a risk uninsurable. (Chapter 4, Risk Management).
2. Vaughan, E. J., & Vaughan, T. (2013). Fundamentals of Risk and Insurance (11th ed.). Wiley. Chapter 2, "The Problem of Risk," lists the "Requisites of an Insurable Risk." Among these are that the loss must be "definite and measurable." The text explains, "It must be possible to

determine that a loss has taken place, and it must be possible to measure the value of the loss." This directly supports why option B describes an uninsurable risk. (pp. 26-27).
3. ASIS International. (2021). Protection of Assets (POA), Business Principles. This foundational text for the CPP exam details the principles of risk management. In the section on Risk Treatment/Mitigation, the criteria for transferring risk via insurance are explained. A key criterion is that the loss must be quantifiable and tied to a specific event, without which an insurance contract cannot be properly structured or executed. (Risk Management volume, Section on Risk Transfer).

Question: 26

In order to dissipate heat, a records safe must contain insulation and:

A. moisture.

B. laminated steel.

C. vacuum.

D. carbon.

Answer:

A

Explanation:

Fire-resistant records safes are engineered to protect their contents from high temperatures. The primary mechanism for this, besides the insulating material itself, is the presence of chemically-bound moisture within the insulation. When the safe is exposed to the heat of a fire, this moisture is released as steam. The process of converting water to steam, known as the latent heat of vaporization, absorbs a significant amount of thermal energy. This "steaming" effect actively cools the safe's interior, keeping the temperature below the charring point of paper (approximately 177C / 350F) for a specified duration.

Why Incorrect Options are Wrong:

B. laminated steel. Laminated steel is primarily used to enhance a safe's resistance to physical (burglary) attacks, not for heat dissipation.
C. vacuum. A vacuum is an excellent insulator that prevents heat transfer, but it is not a practical design for safes and does not actively dissipate heat like the steaming process.
D. carbon. While some specialized fire-resistant materials may contain carbon, it is not the primary agent for heat dissipation in standard record safes; moisture is the key component.

References:

1. Fennelly, L. J. (Ed.). (2021). Protection of Assets: Physical Security. ASIS International. Chapter 5, "Barriers, Locks, and Safes," Section: "Fire-Resistive Safes and Containers." The text explains that the insulation in fire-rated safes contains moisture that turns to steam to absorb heat and protect the contents.
2. Underwriters Laboratories. (2016). UL 72: Standard for Tests for Fire Resistance of Record Protection Equipment. Section 1.1. This standard's testing protocol is based on a safe's ability to limit the internal temperature rise, a performance characteristic achieved by designs incorporating moisture-releasing insulation that creates steam.
3. Garcia, M. L. (2008). The Design and Evaluation of Physical Protection Systems (2nd ed.). Butterworth-Heinemann. Chapter 4, "Delay," pp. 85-86. The book discusses the construction of

fire-resistant containers, noting the use of materials like gypsum that release water vapor when heated to keep internal temperatures low.

Question: 27

An essential first step in developing the security department budget is to:

A. gather specific cost information.

B. estimate the department's share of the overall corporate budget.

C. determine minimum staffing levels.

D. review the corporation's overall strategy and goals.

Answer:

D

Explanation:

The foundational principle of effective security management is its alignment with the organization's strategic objectives. The security department's budget is a financial plan designed to support its mission, which in turn must support the overall corporate mission. Therefore, the essential first step is to review and understand the corporation's strategy and goals. This ensures that security resources are allocated to protect the assets and processes most critical to the organization's success, making the budget relevant, justifiable, and value-driven. All other budgeting activities are subsequent to this strategic alignment.

Why Incorrect Options are Wrong:

A. Gathering specific cost information is a tactical step performed only after security requirements, which are derived from corporate goals, have been defined.
B. Estimating a share of the corporate budget is a reactive, top-down approach that may not reflect the actual security needs required to support business objectives.
C. Determining minimum staffing levels is a component of the budget, but it must be based on the services needed to achieve security objectives aligned with corporate strategy.

References:

1. ASIS International. (2021). Protection of Assets (POA), Business Principles. Alexandria, VA: ASIS International. The section on Financial Management emphasizes that a budget is the financial expression of a plan, and the plan must be derived from the organization's goals and objectives. The process begins with understanding the business context.
2. Sennewald, C. A., & Baillie, C. (2020). Effective Security Management (7th ed.). Butterworth-Heinemann. In Chapter 10, "Budgeting for Security," it is stated, "The security budget must be based on the needs of the organization... The security manager must understand the organization's mission, goals, and objectives to develop a budget that supports them." (p. 121).
3. Fischer, R. J., Halibozek, E., & Green, G. (2022). Introduction to Security (11th ed.). Butterworth-Heinemann. Chapter 4, "Management of Security," discusses the necessity for

security managers to align their department's functions and financial planning with the broader business objectives to demonstrate value and gain support.

Question: 28

A policy for the protection of company-sensitive information must:

A. require employees to sign a nondisclosure agreement.

B. identify at least three distinct levels of sensitive information.

C. require employees to sign a noncompetitive statement.

D. provide guidelines that specifically identify the protected information.

Answer:

D

Explanation:

The fundamental purpose of a policy is to establish management's intent and provide guidance. For a policy on protecting sensitive information to be effective, enforceable, and understandable, it must first clearly define the scope of what is being protected. Without specific guidelines that identify the information assets covered by the policy (e.g., financial records, intellectual property, customer data), employees cannot be held accountable for protecting them, and the policy itself becomes ambiguous and impractical. This identification is the foundational element upon which all other protective measures, procedures, and controls are built.

Why Incorrect Options are Wrong:

A. A nondisclosure agreement is a legal mechanism used to enforce a policy, not a mandatory component of the policy document itself.
B. Classifying information into multiple levels is a best practice for risk management but not a universal requirement for a policy to be valid.
C. A non-compete agreement is a separate legal contract concerning post-employment activities and is distinct from an information protection policy.

References:

1. ASIS International. (2021). Protection of Assets: Information Security. Alexandria, VA: ASIS International. In the chapter on Information Security Governance, the development of security policies is detailed. It is a core principle that a policy must clearly define its scope, which includes identifying the specific information assets and data types that the policy is intended to protect (Chapter 2, Section: "Policy, Standards, and Guidelines").
2. Fischer, R. J., Halibozek, E., & Walters, D. C. (2019). Introduction to Security (10th ed.). Butterworth-Heinemann. In Chapter 15, "Information Security," the text states that an effective information security policy must "define what information is considered sensitive and proprietary" to provide clear direction to employees (p. 385).
3. Peltier, T. R. (2013). Information Security Policies, Procedures, and Standards: A Practitioner's

Reference. Auerbach Publications. Chapter 3, "Developing and Implementing Security Policies," emphasizes that a critical early step is to identify and inventory information assets. The policy document must then explicitly define the types of information to be protected to be effective (Section 3.2, "Policy Development Life Cycle"). DOI: https://doi.org/10.1201/b15782

Question: 29

When assessing risk in an enterprise's macro environment, regulatory policies, and other legal constraints on a business or industry are examples of:

A. political risk

B. financial risk

C. economic risk.

D. institutional risk.

Answer:

A

Explanation:

Regulatory policies and legal constraints are direct results of governmental and legislative actions. In the context of macro-environmental risk assessment, these factors are classified as political risks. Political risk encompasses the potential for government actions, changes in policy, legislative changes, or regulatory frameworks to negatively impact an enterprise's profitability or operations. Analyzing these elements is a fundamental component of understanding the political landscape in which a business functions.

Why Incorrect Options are Wrong:

B. financial risk: This pertains to a company's capital structure, credit, liquidity, and market fluctuations (e.g., interest rates), not the governmental policies that may influence them.
C. economic risk: This relates to broader macroeconomic factors such as inflation, recession, currency exchange rates, and GDP growth, rather than specific laws or regulations.
D. institutional risk: This is a broader concept concerning the stability and quality of a country's formal and informal institutions (e.g., legal system, property rights), but political risk is the more precise term for specific government policies.

References:

1. ASIS International. (2021). Protection of Assets: Security Management. Alexandria, VA: ASIS International. In the chapter on "Global Business Environment," the PESTLE (Political, Economic, Social, Technological, Legal, and Environmental) analysis model is discussed. The 'Political' and 'Legal' components explicitly cover government policy, political stability, tax policy, labor law, and other regulations that constrain business, which are all forms of political risk. (Section on Strategic Planning and the External Environment).
2. An, H., & Chen, Y. (2021). The effect of political risk on corporate risk-taking: A literature review. Finance Research Letters, 43, 101978. https://doi.org/10.1016/j.frl.2021.101978. This academic review defines political risk as stemming from "government actions which interfere with

or prevent business transactions, or change the terms of agreements, or cause the confiscation of wholly or partially-owned business property," directly linking government policy and regulation to the concept. (Section 1. Introduction).
3. Rice, G., & Zeglat, D. (2012). The Process of Risk Management in an International Context. In Global Business: An Economic, Social, and Environmental Perspective. The Saylor Foundation. This university-level text states, "Political risk refers to the political forces and government actions that could negatively affect a company's operations and profits." It lists examples such as changes in regulations and legal constraints. (Chapter 11, Section 11.2).

Question: 30

Which of the following statements correctly applies to the Theory X type of management?

A. Humans work only to satisfy basic needs.

B. Punishment or the threat of punishment is an effective management technique.

C. The average human seeks responsibility and job satisfaction.

D. Work is as natural as play or rest.

Answer:

B

Explanation:

Douglas McGregor's Theory X posits that the average employee is inherently lazy, dislikes work, and will avoid it if possible. Consequently, Theory X managers believe that to achieve organizational goals, workers must be coerced, controlled, directed, and threatened with punishment. This authoritarian management style assumes that external control and the threat of negative consequences are the primary motivators for employees, making punishment or its threat a central and effective technique within this framework.

Why Incorrect Options are Wrong:

A. Humans work only to satisfy basic needs.
This describes the motivational assumption behind Theory X (related to Maslow's lower-order needs), but B describes the actual management technique applied, which is more specific to the question.
C. The average human seeks responsibility and job satisfaction.
This is a core assumption of Theory Y, which presents a more optimistic and participative view of employees.
D. Work is as natural as play or rest.
This is a fundamental tenet of Theory Y, directly contradicting the Theory X assumption that people inherently dislike work.

References:

1. ASIS International. (2021). Protection of Assets (POA), Business Principles. Alexandria, VA: ASIS International. In the chapter on "Management and Leadership," the section on "Theories of Motivation" explicitly states that under Theory X, "most people must be coerced, controlled, directed, and threatened with punishment to get them to put forth adequate effort toward the achievement of organizational objectives."
2. McGregor, D. (1960). The Human Side of Enterprise. McGraw-Hill. In Chapter 3, "Theory X: The Traditional View of Direction and Control," McGregor outlines the core proposition that

management must use threats and coercion because of the average human's inherent dislike for work (pp. 33-34).
3. Carson, C. M. (2005). A historical view of Douglas McGregor's Theory Y. Management Decision, 43(3), 450-460. https://doi.org/10.1108/00251740510589814. This article reviews McGregor's original work, reaffirming that Theory X is characterized by a management style of "coercion and control" (p. 452).