DUMPSARENA

Physical Security Professional(PSP)Exam

ASIS ASIS-PSP

Version Demo

Total Demo Questions: 31

Total Premium Questions: 390

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Physical Security Assessment	123
Topic 2, Application, Design, and Integration of Physical Security Systems	115
Topic 3, Implementation of Physical Security Measures	132
Topic 4, Mix Questions	20
Total	390

QUESTION NO: 1

Which of the following consumes the greatest portion of a project manager's time over the life of a project?

A. Documentation

B. Meetings

C. Planning

D. Control

ANSWER: D

Explanation:

Control consumes the greatest portion of a project manager's time because it is a continuous responsibility throughout project execution and continues until formal closeout. Project control involves measuring actual performance against the approved scope, schedule, budget, quality requirements, and risk responses; identifying variances; determining whether corrective or preventive action is needed; managing approved changes; and reporting reliable status to stakeholders. These activities recur as work progresses rather than being completed once at the beginning or end of the effort. Effective control also keeps the physical-security project aligned with the owner's operational requirements and ensures that deviations are addressed before they affect project objectives or acceptance. In recognized project-management practice, monitoring and controlling is an integrated, ongoing process group that interacts with the work being performed and supplies the information needed for informed decisions. The Project Management Institute describes monitoring and controlling as tracking, reviewing, and regulating project progress and performance, including identifying areas where plan changes are required. This continuous oversight is why control represents the largest sustained demand on the project manager's time across the project life cycle. See the Project Management Institute's discussion of monitoring and controlling project work and PMI's overview of project-management responsibilities.

QUESTION NO: 2

When yard space and warehousing is required even in urban areas, _____ is the boundary of the property owned by the company.

A. Fence

B. Wall

C. Perimeter

D. Chain link

ANSWER: C

Explanation:

Perimeter is correct because it denotes the outer boundary that defines the extent of a company's site or property. In physical-security planning, the perimeter is the line—whether legally defined, physically marked, or both—at which the organization's controlled property begins and the surrounding public or neighboring area ends. A site that includes urban warehousing and yard space still requires a clearly identified perimeter so security practitioners can assess exposure, establish protection objectives, and organize access-control and intrusion-detection measures around the property boundary.

The perimeter is a foundational concept in layered security. Its definition informs the placement and design of protective measures such as vehicle and pedestrian entry points, lighting, surveillance coverage, signage, fencing, and detection systems. The specific boundary treatment may differ according to site conditions, risk assessment findings, operational needs, applicable regulations, and the desired delay and deterrence performance. Thus, the term refers to the boundary itself rather than to a particular construction material or barrier type. This is consistent with federal physical-security guidance, which treats site perimeter protection as a key element of facility security planning. See the CISA Physical Security Performance Goals for Facilities and the Interagency Security Committee criteria.

QUESTION NO: 3

An employee with access to sensitive areas is involuntarily terminated. Which two actions should be completed promptly to reduce the risk of unauthorized re-entry? Select two.

A. Deactivate the employee's access-control privileges.

B. Recover issued badges, keys, and other access devices.

C. Reprogram every reader at the facility.

D. Retain access privileges until the next payroll cycle ends.

ANSWER: A B

Explanation:

Revoking physical access privileges and recovering organization-issued credentials and keys are correct because they directly prevent continued use of access rights and accountable security assets. A termination process should also include appropriate notification and documentation. Reprogramming all readers is not normally necessary when individual credentials can be deactivated, and retaining access until the end of the next payroll cycle creates an unnecessary exposure.

QUESTION NO: 4

A security manager is developing post orders for officers assigned to a high-value storage area. Which two items should be included to support consistent and lawful performance? Select two.

A. Required patrol, observation, communication, and incident-reporting duties

B. Limits of authority and procedures for requesting supervisory or police assistance

C. Authorization to disregard written policy when workload is high

D. Responsibility for independently interpreting all applicable criminal law

ANSWER: A B

Explanation:

Post orders should define the officer’s duties, reporting requirements, and actions for foreseeable incidents, and they should identify the limits of authority and escalation procedures. These directions connect organizational policy to the officer’s assigned post and promote consistent decisions. Instructions to disregard written policy or to determine legal authority independently would create unacceptable inconsistency and legal risk.

QUESTION NO: 5

A security manager is preparing an after-action review following a major access-control outage. Which two actions are MOST important for ensuring that the review leads to measurable improvement? Select two.

A. Compare actual actions and timelines with established procedures.

B. Assign corrective actions to responsible owners with completion dates.

C. Close the review when the initial incident report is filed.

D. Rely solely on informal opinions gathered after the event.

ANSWER: A B

Explanation:

Comparing actual performance with established procedures and assigning corrective actions with responsible owners and completion dates are correct. These actions turn observations into accountable improvements. Collecting unverified opinions without reconstructing the event, or closing the review after the incident report is filed, does not demonstrate that identified weaknesses will be addressed.

QUESTION NO: 6

The prediction of internal crime relies most heavily on analysis of:

A. Employee background checks

B. Critical area surveillance

C. Employee surveys

D. Historical data

ANSWER: D

Explanation:

Historical data is the strongest basis for predicting internal crime because prediction depends on identifying recurring conditions, patterns, and indicators from prior events. Security incident records, loss reports, investigation findings, audit exceptions, access-control activity, inventory discrepancies, and reports of misconduct can be analyzed to establish trends by location, time, asset type, work process, or role. This analysis helps the security professional recognize where opportunities for theft, fraud, sabotage, or other insider misconduct are most likely to develop and to direct preventive controls and investigative resources accordingly. It also supports risk assessment by turning individual events into measurable information about frequency, impact, and common contributing conditions. Effective crime analysis is therefore not merely a recordkeeping activity; it is a proactive process that uses past and current information to forecast likely future problems and prioritize treatment strategies. ASIS guidance on physical asset protection emphasizes using risk assessment and relevant organizational information to identify threats and vulnerabilities, while CISA's insider-threat resources similarly stress the value of observable data and reporting in recognizing insider-risk indicators. See ASIS Standards and Guidelines and CISA Insider Threat Mitigation.

QUESTION NO: 7

A new research and development center is being planned. At what point in the project should the security manager become involved?

A. Equipment specification and bid phase

B. Completion of the preliminary architectural drawings

C. Initial design phase

D. Concept presentation to senior management

ANSWER: C

Explanation:

Initial design phase is correct because security must be integrated while fundamental facility decisions remain flexible. At this stage, the security manager can translate the organization's risk profile and operational requirements into design criteria affecting site selection and layout, building orientation, perimeter definition, access and circulation patterns, zoning, protected-area locations, security-control spaces, communications pathways, and allowances for future systems. For a research and development center, early attention is particularly important because intellectual property, sensitive prototypes, personnel safety, and controlled visitor access may require layered protection and carefully separated circulation routes.

Early involvement also enables security requirements to be coordinated with architectural, engineering, life-safety, information-technology, and operational requirements rather than being added as isolated equipment later. This supports a risk-based, defense-in-depth approach and avoids costly redesign when structural, electrical, network, and space-planning decisions are already fixed. The U.S. Cybersecurity and Infrastructure Security Agency's Interagency Security Committee resources emphasize incorporating threat and risk considerations into facility design decisions; see its Design-Basis Threat Report. ASIS guidance likewise recognizes that physical-security planning should be integrated with the facility and organizational environment from the outset; see ASIS Standards and Guidelines.

QUESTION NO: 8

A facility is replacing its mechanical key-control program after discovering that several keys cannot be accounted for. Which two controls would MOST directly strengthen accountability for keys issued to employees? Select two.

A. Require a documented issue-and-return record for each key

B. Periodically reconcile issued keys with authorized keyholders

C. Increase the number of master keys available to supervisors

D. Store spare keys in an unlocked desk near the security office

ANSWER: A B

Explanation:

A documented issue-and-return process and periodic reconciliation of issued keys to authorized holders directly establish accountability. These controls create a record of possession and help identify missing, unreturned, or improperly issued keys. Increasing the number of master keys increases exposure if a key is lost or copied. Storing spare keys in an unlocked desk removes control rather than strengthening it.

QUESTION NO: 9

A primary ingredient that represents the loss prevention specialist's opportunity to reduce theft is called:

A. Low deterrence

B. Confusion

C. Common denominator

D. Reduced Pilfering

ANSWER: C

Explanation:

Common denominator is correct because, in loss-prevention practice, it identifies the shared, recurring condition that creates an opportunity for theft or other loss. The condition may be a process weakness, insufficient accountability, weak access control, an unobserved area, inconsistent inventory handling, or another vulnerability that appears across incidents. Its value to the loss prevention specialist is practical: once the common condition is recognized through incident reports, audits, observations, and loss data, controls can be directed at that condition to reduce the opportunity for future theft.

This approach is consistent with physical-security risk management. A professional identifies assets, threats, vulnerabilities, and the controls needed to reduce risk; repeated loss events should therefore be examined for the underlying factor they share. Addressing that factor through improved procedures, supervision, environmental design, access restrictions, inventory controls, or monitoring can prevent recurrence rather than merely responding to individual incidents. ASIS describes the PSP credential as encompassing physical-security assessment, application, and evaluation, which supports this systematic identification and treatment of vulnerabilities. See ASIS Physical Security Professional (PSP) and the CISA physical security resources.

QUESTION NO: 10

Which type of lamp emits a strong light with a bluish cast?

A. Sodium vapor

B. Metal halide

C. Mercury vapor

D. Incandescent

ANSWER: C

Explanation:

Mercury vapor is the correct answer because mercury-vapor discharge lamps characteristically produce an intense, cool bluish to blue-green light. An electric arc passes through mercury vapor in the lamp's arc tube, creating a high-intensity discharge that is well suited to large-area and exterior illumination applications. The visual appearance of the source is an important operational characteristic in physical-security lighting: its cool, bluish cast distinguishes mercury-vapor lighting from sources that produce warmer or more neutral white illumination. The lamp's spectrum is dominated by mercury emission lines, which accounts for the distinctive color appearance and historically limited its color-rendering performance compared with more modern alternatives. In a security-lighting context, identifying the source by its emitted color helps personnel recognize the expected lighting quality and potential effects on observation and camera imaging. The Edison Tech Center's technical overview describes mercury-vapor lamps as high-intensity-discharge sources and discusses their characteristic blue-green output: Mercury Vapor Lamps. The U.S. Department of Energy also identifies mercury-vapor lighting as a type of high-intensity-discharge lighting in its overview of lighting technologies: Lighting Choices to Save You Money.

QUESTION NO: 11

Private sector will become increasingly involve in crime prevention; public law enforcement will then be free to concentrate more heavily on violent crimes and crime response.

A. True

B. False

ANSWER: A

Explanation:

The statement is true. A central feature of contemporary physical security practice is the expanding role of private-sector organizations in preventing loss, deterring crime, protecting facilities and assets, managing access, conducting security investigations, and sharing relevant information with public law-enforcement partners. This is often described as the "pluralization" of policing: public police remain responsible for their statutory law-enforcement mission, while private security resources address many preventive and protective functions at privately owned locations and in commercial environments.

When trained private-security personnel and organizational security programs provide effective prevention, observation, reporting, initial incident management, and coordination with police, public law enforcement can direct finite personnel and specialized investigative resources toward priority public-safety demands, including serious violence, emergency response, and complex criminal investigations. This relationship does not transfer police powers to private security; rather, it emphasizes complementary responsibilities, clear procedures, lawful information sharing, and coordinated response protocols. ASIS's Professional Certified Investigator and Physical Security Professional bodies of knowledge recognize crime prevention and collaboration with law enforcement as important elements of organizational security practice. See ASIS's overview of the PSP certification at ASIS Physical Security Professional (PSP) and the U.S. Department of Justice discussion of public-private partnerships at National Institute of Justice: Public-Private Partnerships.

QUESTION NO: 12

Which of the following is NOT the activity and concern of a crisis management plan?

A. Crisis management team

B. Disaster operation

C. Media operation

D. Vital records

ANSWER: D

Explanation:

Vital records are not principally an activity or concern of a crisis management plan. Crisis management provides the executive-level framework for directing an organization through a disruptive event: establishing authority, activating the crisis-management organization, coordinating emergency decisions and resources, maintaining situational awareness, and communicating with employees, responders, stakeholders, and the public. The plan therefore concentrates on how leaders organize, make timely decisions, and manage the consequences of an incident.

Vital records management, by contrast, is a records-protection and continuity capability. It identifies records and information essential to protecting legal and financial rights, sustaining critical functions, and resuming operations after an emergency; it also addresses their protection, accessibility, backup, and recovery. Those controls support organizational resilience and business continuity, and crisis leaders may rely on vital information during an incident, but the detailed management of such records is not itself a core crisis-management-plan function. FEMA's planning doctrine describes incident planning as an integrated process for coordinating actions and resources, while the U.S. National Archives defines and addresses vital records as records needed to continue operations or protect rights following an emergency. See FEMA's Comprehensive Preparedness Guide 101 and National Archives guidance on vital records.

QUESTION NO: 13

As part of business continuity planning, a business impact analysis is being completed for a security operations function. Which two outputs would be MOST useful for developing recovery strategies? Select two.

A. Prioritized recovery requirements for time-sensitive functions

B. Dependencies on personnel, facilities, technology, and suppliers

C. A determination of individual responsibility for a prior incident

D. A final selection of a security-system manufacturer

ANSWER: A B

Explanation:

Recovery priorities and resource dependencies are correct outputs because they identify which functions must be restored first and the personnel, facilities, technology, communications, and suppliers needed to restore them. A business impact analysis evaluates the consequences of disruption over time; it does not replace incident investigation or select a particular security-system manufacturer.

QUESTION NO: 14

Document the events, circumstances, and chronology and prepare a "lesson learned" review are the primary parts of:

A. Testing

B. Quality assurance

C. After action

D. All of the above

ANSWER: C

Explanation:

After action is correct because an after-action review is the formal post-incident or post-exercise process used to capture what occurred, establish the sequence of events and operating conditions, evaluate the response, and identify lessons that should drive corrective actions. In physical-security practice, this review creates an accountable record of the event while turning observations into improvements to plans, staffing, training, communications, technology, and response procedures. A useful after-action process does more than collect narrative reports: it reconstructs the chronology, compares performance with objectives and established procedures, identifies improvement items, assigns responsibility, and tracks those items through completion. This supports organizational resilience by ensuring that a security incident, emergency, or exercise produces measurable enhancements rather than simply being closed out administratively. The U.S. Department of Homeland Security's exercise doctrine describes after-action reporting as documenting strengths and areas for improvement and connecting them to an improvement plan. Similarly, CISA emphasizes evaluating exercise performance and using findings to improve preparedness. These concepts align directly with documenting events, circumstances, chronology, and lessons learned. See FEMA Homeland Security Exercise and Evaluation Program doctrine and CISA's HSEEP resource.

QUESTION NO: 15

Which of eth following is NOT the type of insurance?

A. Fidelity Bonds

B. Surety Bonds

C. 3-D policies

D. Privacy Invasion

ANSWER: D

Explanation:

Privacy Invasion is correct because it describes a potential legal harm or liability exposure, rather than the name of an insurance product or bond category. In a physical-security context, an organization may face an invasion-of-privacy allegation when surveillance, access-control records, searches, personal-information handling, or monitoring practices improperly intrude on an individual's privacy rights. The resulting exposure can include defense costs, settlements, judgments, regulatory action, and reputational harm. Risk managers address this exposure by identifying the applicable activities and selecting coverage that may respond to the particular claim, such as general liability coverage containing relevant personal-injury provisions, employment-practices liability coverage, media liability coverage, or cyber/privacy liability coverage. Coverage depends on the policy wording, exclusions, jurisdiction, and facts of the incident; "Privacy Invasion" itself is not a standalone, conventional insurance classification. This distinction is important for PSP professionals because insurance and bonds are risk-transfer mechanisms, whereas invasion of privacy is a risk event that security policies and operational controls should help prevent. The National Association of Insurance Commissioners discusses privacy-related exposures within cyber insurance at NAIC Cyber Risk. The U.S. Department of Justice also describes privacy protections and related legal considerations at Privacy Act of 1974.

QUESTION NO: 16

Following a prolonged utility outage, a facility's access-control system operated on backup power but security officers had difficulty controlling entry because the visitor-management workstation was unavailable. Which two actions should be included in the corrective-action plan? Select two.

A. Develop a documented manual procedure for visitor verification, logging, and escorting

B. Exercise an alternate method for maintaining visitor-management capability during an outage

C. Replace all access-control readers with mechanical locks

D. Suspend visitor screening until the workstation becomes available

ANSWER: A B

Explanation:

A documented manual visitor-control procedure and an exercised continuity arrangement for the visitor-management function address the demonstrated operational gap. The facility needs a reliable method to verify, record, escort, and account for visitors when the normal workstation is unavailable. Replacing all access-control readers does not address the loss of visitor-processing capability, and eliminating visitor screening would increase risk during a disruption. Corrective actions should address the specific failed dependency and be validated through training or exercises.

QUESTION NO: 17

A physical security project is approaching final acceptance. Which two actions are MOST important before the owner accepts an integrated access-control and video-surveillance system? Select two.

A. Conduct functional testing against the approved acceptance criteria

B. Obtain as-built drawings, operating instructions, and warranty documentation

C. Select the preferred manufacturer for future system expansion

D. Reevaluate competing bids received during the procurement phase

ANSWER: A B

Explanation:

Functional testing against documented acceptance criteria and receipt of complete closeout documentation are essential before acceptance. Testing confirms that the installed system performs the required functions, including interfaces and alarm workflows. Documentation such as as-built drawings, device schedules, operating instructions, and warranty information enables the owner to operate and maintain the system after turnover. Selecting a future upgrade path or comparing the contractor's original bid with competitors' bids may be useful management activities, but neither confirms that the delivered system meets the contractual requirements.

QUESTION NO: 18

A security survey of a distribution centre identifies repeated losses from the employee parking area after dark. Which two findings would MOST directly support a recommendation for improved natural surveillance? Select two.

A. Overgrown landscaping obstructs views between the building and parking spaces

B. Pedestrian routes from the parking area have inadequate illumination

C. Vehicle inventory records are retained for less than one year

D. The loading dock has six overhead doors

ANSWER: A B

Explanation:

Overgrown landscaping that obstructs sightlines and inadequate illumination at pedestrian routes both directly limit the ability of legitimate users, guards, and cameras to observe activity in the parking area. Correcting these conditions supports natural surveillance by improving visibility and reducing concealment opportunities. A documented vehicle inventory process and the number of loading-dock doors may be relevant to other security concerns, but neither finding directly establishes a natural-surveillance deficiency in the employee parking area.

QUESTION NO: 19

The contingency fee component of a bid package represents what percentage of the total cost figure?

A. 5%

B. 10%

C. 15%

D. 20%

ANSWER: B

Explanation:

10% is the correct contingency-fee component for the total cost figure in this bid-package context. A contingency is a planned allowance incorporated into the project estimate to address uncertain but reasonably foreseeable costs that may arise as work proceeds, such as minor scope refinements, field conditions, coordination needs, price variability, or implementation issues. Including this allowance supports a more realistic and defensible project budget rather than treating every unexpected requirement as an unplanned overrun. In physical-security projects, the bid package should present a clear total project figure that accounts for the practical uncertainty inherent in deploying integrated equipment, infrastructure, installation labor, and associated project activities. The 10% convention supplies a meaningful reserve while retaining a budget figure suitable for planning, approval, and procurement purposes. Contingency should be identified and managed as part of sound cost estimating and risk management, with its use governed through the project's established authorization process. The U.S. Government Accountability Office explains that reliable cost estimates address risk and uncertainty through risk analysis and contingency reserves; see its Cost Estimating and Assessment Guide. Related project-management guidance on managing uncertainty and risk is available from the Project Management Institute.

QUESTION NO: 20

The balanced magnetic switch differs from the simple magnetic switch in that it:

A. Is meant to be used on non-ferrous doors such as aluminum or wood

B. Must be mounted at an angle

C. Must be used in pairs

D. Is harder to defeat

ANSWER: D

Explanation:

"Is harder to defeat" is correct because a balanced magnetic switch is specifically designed to provide greater resistance to magnetic tampering than a simple, standard magnetic contact. A conventional magnetic switch typically changes state when its reed switch senses the nearby operating magnet; an intruder may try to hold that switch in its normal condition with another magnet while opening the protected door, window, or similar opening. A balanced magnetic switch uses a more complex magnetic arrangement, commonly involving carefully matched magnet polarity and field strength. The contact is intended to operate only when the proper actuator magnet is in the expected position and orientation. Introducing an external magnet, using the wrong polarity, or moving the actuator away commonly produces an alarm condition rather than preserving the secure state. This makes defeat by magnetic substitution substantially more difficult and supports the objective of detecting unauthorized opening or tampering at a protected opening. In practice, correct installation remains essential: the specified actuator, alignment, gap, and mounting arrangement must be maintained so that the device performs according to its listed operating characteristics. See the Alarm Industry Communications Committee resources for intrusion-alarm industry information and the UL Solutions burglar alarm systems overview for information on alarm-system evaluation and reliability.

QUESTION NO: 21

Which of the following processes should be implemented in addition to a risk assessment when considering how a potentially disruptive event can negatively affect a facility ' s security program?

A. Adversary Route

B. After Action Report

C. Critical Event Review

D. Business Impact Analysis

ANSWER: D

Explanation:

Business Impact Analysis is the appropriate complementary process because it examines the consequences to the organization when a disruptive event occurs. A risk assessment identifies and evaluates threats, vulnerabilities, likelihood, and potential risk; the business impact analysis then determines how interruption of facility operations, security functions, people, technology, information, suppliers, and other dependencies would affect the organization over time. This includes identifying critical activities, establishing maximum tolerable downtime or disruption, determining recovery priorities, and estimating operational, financial, legal, safety, and reputational effects. For a facility security program, these findings help security leaders prioritize continuity and recovery measures for essential capabilities such as access control, communications, incident command, life-safety systems, guard-force operations, and protection of critical assets. The analysis therefore converts the general concern that an event may be disruptive into documented, time-based business consequences and recovery requirements. This is a foundational element of business continuity planning and supports informed allocation of protective and resilience resources. The U.S. Cybersecurity and Infrastructure Security Agency describes business impact analysis as a process for identifying critical functions and the impacts of disruption: CISA Business Continuity Planning. Related continuity-management guidance is available from ISO 22301.

QUESTION NO: 22

A security professional is conducting an initial physical security risk assessment for a newly acquired facility. Which two sources of information would MOST directly support identification of credible threats and vulnerabilities? Select two.

A. Incident and loss-history records for the facility and surrounding area

B. A physical survey of boundaries, access points, and protective measures

C. A catalogue of security equipment available from local suppliers

D. An unverified estimate of future construction costs

ANSWER: A B

Explanation:

Incident-history records and a physical site survey are correct because they provide direct evidence of prior events, existing conditions, access routes, protective measures, and weaknesses that may be exploited. Interviews with knowledgeable facility personnel may supplement these sources, but a general equipment catalogue and an unverified supplier estimate do not establish credible threats or site-specific vulnerabilities.

QUESTION NO: 23

Worms take over computer memory and deny its use to legitimate programs.

A. True

B. False

ANSWER: A

Explanation:

True is correct. A computer worm is self-replicating malicious code that can spread independently across systems or networks. As it executes and creates copies of itself, it may consume memory, processor time, storage, network bandwidth, and other finite system resources. Resource consumption can impair normal application operation and, when severe, cause a denial-of-service condition in which legitimate programs or users cannot obtain the memory or processing capacity they need. This effect does not require the worm to alter a legitimate program; uncontrolled replication and execution alone can exhaust available resources. The precise impact depends on the worm's design and the affected environment, but depletion of system or network resources is a recognized consequence of worm activity and is consistent with the statement. NIST defines a worm as a self-replicating, self-propagating program, while CISA identifies malware—including worms—as a threat that can disrupt systems and operations. See the NIST Computer Security Resource Center definition of a worm and CISA's malware guidance.

QUESTION NO: 24

Based on their ability to meet the needs of an entire organization, which of the following stakeholders is MOST crucial to engage for a successful operation of an asset protection strategy?

A. Security

B. Executives

C. IT Department

D. Human resources

ANSWER: B

Explanation:

Executives are the most crucial stakeholders to engage because an asset protection strategy must operate as an enterprise-wide business program rather than as an isolated security function. Senior executives establish organizational direction, determine risk tolerance, allocate resources, approve policies, and provide the authority needed to coordinate implementation among business units. Their sponsorship also helps ensure that asset-protection objectives support broader organizational priorities, including operational continuity, legal and regulatory responsibilities, financial stewardship, and protection of people, information, and property. Effective executive engagement creates accountability at the appropriate level and enables security leaders to obtain cross-functional participation necessary for consistent execution. ASIS guidance emphasizes that effective security risk management is aligned with organizational objectives and supported by management commitment; this alignment is essential when protection measures affect multiple functions and require sustained resources. Executive leadership therefore provides the strategic oversight and enterprise influence needed for the successful operation of the strategy. See the ASIS Standards and Guidelines and the ASIS Physical Security Professional certification overview.

QUESTION NO: 25

The process of pre-qualifying vendors before issuing the request for proposal (RFP) helps to ensure that:

A. All applicable codes are enforced

B. Only credible and competent vendors bid on the project

C. Only financially secure vendors bid on the project

D. All specifications of the project are met

ANSWER: B

Explanation:

Only credible and competent vendors bid on the project is correct because prequalification is a screening step performed before an RFP is distributed. Its purpose is to develop a shortlist of suppliers that have demonstrated the capacity to perform the work and are suitable candidates for the procurement. Depending on the project, prequalification criteria can address relevant technical experience, past performance, staffing and resources, licenses or certifications, quality-management capability, insurance, financial capacity, and the ability to meet project schedules and contractual requirements. Applying these criteria early helps the security professional direct the RFP to firms that can provide a meaningful, responsive proposal and are realistically capable of delivering the required physical-security solution. This makes the solicitation and subsequent evaluation process more efficient while reducing the risk associated with accepting a proposal from a vendor that lacks the necessary qualifications. Financial strength can be a relevant element of the prequalification review, but vendor credibility and competence encompass the broader purpose of the process. The U.S. General Services Administration describes prequalification as a means of identifying vendors that meet established requirements before competition, and procurement guidance recognizes supplier capability assessment as a key source-selection activity. See GSA contractor responsibilities and FAR 9.104-1, General standards.

QUESTION NO: 26

To deal with the lack of security, both government organizations have developed guidelines for protecting electric facilities and distribution systems. On the private side, the Edison Electric Institute developed guidelines that have been passed on to the North American Electric Reliability Council (NERC), the U.S. Department of Energy's coordinator for the U.S. electrical infrastructure. Among other things the guide lines cover:

A. Vulnerability/risk analysis

B. Threat response

C. Cyber scenario

D. Emergency detection

ANSWER: A B

Explanation:

Vulnerability/risk analysis is correct because effective protection of electric facilities begins by identifying critical assets, evaluating credible threats and vulnerabilities, estimating consequences, and using that information to prioritize proportionate protective measures. This risk-based process is central to electric-sector security planning because generation, transmission, control, and distribution assets have different operational criticality and exposure profiles. **Threat response** is also correct because security guidance must translate assessment results into actionable preparation for, response to, and recovery from threat events. Response planning includes incident coordination, communications, escalation procedures, and the ability to maintain or restore reliable operations following a security incident. These two subjects work together: a vulnerability and risk analysis establishes what requires protection and the relative priority, while threat response establishes how the organization will act when a threat materializes. Current electric-reliability security requirements retain this same approach by requiring responsible entities to identify critical cyber assets, manage security risks, and establish incident-response capabilities. NERC's overview of its Critical Infrastructure Protection standards is available at https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. The U.S. Department of Energy also describes its role in strengthening energy-sector resilience and coordinating response to energy emergencies at https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response.

QUESTION NO: 27

A facility plans to install fixed vehicle barriers near a public entrance. Which two factors are MOST important in determining whether the barrier design is appropriate? Select two.

A. The credible vehicle mass, speed, and approach path

B. The available stand-off distance from the protected asset

C. The preferred colour of the barrier enclosure

D. The landscaping style selected for the entrance

ANSWER: A B

Explanation:

The credible vehicle threat and the barrier's location relative to the protected asset are correct because they determine the required stopping capability, stand-off distance, and placement of the protective measure. A barrier must be selected and installed for the expected vehicle mass, speed, approach path, and consequences of impact. Its colour and landscaping treatment may affect appearance and visibility, but they do not establish whether the barrier provides adequate protective performance.

QUESTION NO: 28

Successful security design recognizes technological developments and integrates:

A. Adversary sequence diagrams, system specifications, and work breakdown structure

B. Threats, operational factors, and likelihood of occurrence

C. Operational factors, organizational needs, and the human element

D. Architectural aspects, security systems, and operational factors

ANSWER: C

Explanation:

Operational factors, organizational needs, and the human element is correct because effective physical security design is a systems-based process rather than simply a selection of current technologies. Operational factors ensure that controls fit actual workflows, staffing, maintenance capabilities, emergency procedures, and site conditions. Organizational needs ensure that the design supports the entity's mission, risk appetite, budget, governance, and continuity requirements. The human element is equally essential: employees, visitors, operators, and response personnel must be able to understand, accept, and use security measures reliably. A technically capable control that disrupts work, creates unsafe workarounds, or cannot be operated consistently will not deliver its intended protection. Integrating these considerations produces layered measures that are practical, sustainable, and aligned with business objectives while accommodating technological change. This integrated, risk-based approach is consistent with the Physical Security Professional body of practice, which emphasizes designing, implementing, and evaluating physical security measures in the context of organizational operations. See ASIS's Physical Security Professional certification overview and the UK National Protective Security Authority's guidance on human factors.

QUESTION NO: 29

Which of the following types of procurement is most frequently used when a customer has intimate knowledge of the requirements defined and the systems available in the market?

A. Invitation to bid

B. Request for proposals

C. Sole source

D. Request for quote

ANSWER: A

Explanation:

Invitation to bid is the appropriate procurement method when the customer has thoroughly defined the required security outcome, equipment or system characteristics, quantities, performance criteria, installation scope, and acceptance requirements, and also understands the available marketplace well enough to specify what is needed without relying on vendors to develop the solution. In this circumstance, the procurement objective is principally to obtain responsive,

comparable bids and select among qualified suppliers using stated criteria, commonly with price as a major factor. A clear, complete bid package enables each bidder to price substantially the same scope, supports fair competition, and reduces the risk that proposals will differ materially in technical approach or assumptions. This aligns with the formal sealed-bidding model: it is suitable where requirements can be described clearly and accurately, competition is expected, and award can be made on the basis of submitted bids. For a physical-security project, this may include a well-engineered access-control, video-surveillance, fencing, or intrusion-detection deployment for which the organization has established specifications and knows that multiple market sources can meet them. The U.S. acquisition regulations describe sealed bidding as appropriate when complete, adequate, and realistic specifications are available and award can be made based on price and price-related factors; see FAR 6.401 and FAR 14.101.

QUESTION NO: 30

An offense punishable by death or by imprisonment for a term exceeding one year is called:

A. Corruption

B. Felony

C. Misguidance

D. Misdemeanor

ANSWER: B

Explanation:

Felony is correct. In the federal criminal-law framework, a felony is an offense for which the authorized punishment is death or imprisonment for more than one year. This classification concerns the maximum punishment authorized by law for the offense, rather than the sentence that a particular defendant ultimately receives. The definition is particularly relevant to security professionals because criminal-offense classifications may affect incident reporting, liaison with law enforcement, background-screening criteria, evidence preservation, and organizational risk decisions. Although terminology and charging practices can vary among state and local jurisdictions, the death-or-more-than-one-year threshold is the standard federal definition and is the intended classification in this question. Title 18 of the U.S. Code expressly defines a felony as an offense punishable by death or imprisonment for a term exceeding one year. The Federal Bureau of Investigation also uses this threshold in describing felony offenses for criminal-history and related justice-system purposes. See 18 U.S.C. § 3559 and the FBI Identity History Summary Checks information page.

QUESTION NO: 31

Effective protective systems integrate each of the following supporting elements except:

A. The assets to be protected, the threat to those assets, and the applicable risk levels

B. Terrorism countermeasures that protect assets against terrorist attacks

C. Procedural security measures including procedures in place before an incident and those used in response to an incident

D. Physical protective measures including barriers, lighting, and electronic security systems

ANSWER: B

Explanation:

Terrorism countermeasures that protect assets against terrorist attacks is the exception because it is a threat-specific security treatment rather than a universal supporting element of every effective protective system. Protective-system design begins with a risk-based understanding of what must be protected, the threats and hazards that could affect it, and the level of risk the organization is prepared to manage. Controls are then selected and integrated in a manner proportionate to that assessment. Counterterrorism measures may be highly appropriate where terrorism is a credible, relevant threat, such as at certain critical-infrastructure sites, prominent venues, or facilities with particular symbolic or operational significance. Their inclusion, however, depends on the documented threat and risk context; they are not inherently required for all organizations

or all facilities. This risk-based approach ensures that protective resources address the organization’s actual exposure and security objectives rather than applying specialized measures by default. ASIS guidance and standards resources emphasize structured, risk-informed security management, while CISA’s risk-assessment methodology similarly frames protective decisions around identified threats, vulnerabilities, and consequences. See ASIS Standards and Guidelines and CISA Risk Assessment Methodology.