PassQueen
a.k.a dumpsqueen.com

Planning & Scheduling Professional (PSP) Exam

ASIS PSP

Version Demo

Total Demo Questions: 45

Total Premium Questions: 450

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Physical Security Assessment	85
Topic 2, Application, Design, and Integration of Physical Security Systems	57
Topic 3, Implementation of Physical Security Measures	269
Topic 4, Mix Questions	39
Total	450

QUESTION NO: 1

The number of security personnel required is generally inversely proportional to the size of the facility, expressed both in terms of square footage or acreage and the number of employees involved.

A. True

B. False

ANSWER: B

Explanation:

False is correct because security staffing is determined through a risk-based assessment of the protection mission and workload, not through an inverse relationship to facility size or population. As a facility's square footage, acreage, occupied buildings, entry points, operating hours, workforce, visitor volume, and protected assets increase, the security program commonly needs greater coverage and more resources to perform access control, patrol, alarm response, incident management, and supervision. Staffing needs may also be affected by threat conditions, crime patterns, the criticality of operations, technology deployment, outsourcing, and the required response-time objective. A larger site or larger employee population does not automatically produce a fixed staffing ratio, but it generally expands the scope of security responsibilities rather than reducing it. The appropriate number of personnel should therefore be supported by a documented security risk assessment, operational requirements, post orders, and coverage calculations. This risk-based approach is consistent with ASIS guidance on protecting assets and managing security programs; see ASIS Standards and Guidelines and the ASIS Protection of Assets resource.

QUESTION NO: 2

Which of the following are appropriate objectives of a post-incident security review?

A. Determining the sequence of events

B. Evaluating the performance of protective measures

C. Assigning blame before the facts are established

D. Identifying corrective actions

E. Capturing lessons learned

ANSWER: A B D E

Explanation:

Determining the sequence of events, **evaluating the performance of protective measures**, **identifying corrective actions**, and **capturing lessons learned** are correct. A post-incident review examines what occurred, how the organization's people, procedures, and technology performed, and what improvements are needed to reduce the likelihood or consequences of a similar event. The review should be factual, documented, and directed toward improving future readiness.

Assigning blame before the facts are established is not an appropriate primary objective. Accountability may be addressed through a separate, fair process when warranted, but the security review should first preserve evidence, establish facts, assess performance, and recommend improvements. FEMA describes after-action reporting as a process for documenting strengths, areas for improvement, and corrective actions. See FEMA Homeland Security Exercise and Evaluation Program.

QUESTION NO: 3

_____ builds on confusion when two or more people take advantage of their positions and the confusion to steal.

A. Conspiracy

B. Accountability

C. Invoicing

D. Proliferation

ANSWER: A

Explanation:

Conspiracy is correct because it involves coordinated action by two or more individuals who use a shared plan to commit an unlawful act, such as theft or fraud. In a physical-security and loss-prevention setting, conspirators may exploit their access, assigned duties, knowledge of procedures, and the uncertainty created when responsibilities overlap. Their coordinated conduct can make theft more difficult to identify because each participant may perform only part of the activity, obscure records, or create conditions in which an irregularity appears to be an ordinary operational error. The essential feature is the agreement and joint effort to achieve the improper objective; the theft may be carried out through multiple acts and by people in different positions. This concept supports the need for security controls that establish clear accountability, separation of duties, supervision, and reliable audit trails. These measures help reveal patterns that indicate coordinated misuse of authority or assets. The U.S. Department of Justice describes conspiracy as an agreement involving two or more persons to commit an offense, with an act in furtherance of that agreement where required. See the U.S. Department of Justice Criminal Resource Manual and ASIS's security standards and guidelines resources.

QUESTION NO: 4

The characteristic of the precedence diagramming method that models construction projects differently than the arrow diagramming method is that it_____.

A. uses arrows to signify logic in a network

B. allows more than one critical path to be represented

C. can be used to calculate the late start and late finish of all activities

D. allows multiple relationship types to be associated with activities

ANSWER: D

Explanation:

The correct answer is **allows multiple relationship types to be associated with activities**. Precedence diagramming method (PDM), also called activity-on-node diagramming, represents activities as nodes and connects them using logical relationships. This gives schedulers the flexibility to model all four standard dependency types: finish-to-start, finish-to-finish, start-to-start, and start-to-finish. Leads and lags can also be applied to these relationships, allowing the schedule to represent realistic overlaps, coordination points, commissioning sequences, and phased construction work.

For example, installation work may start only after design work has started, while testing may need to finish at the same time as installation finishes. Such relationships can be expressed directly in PDM. This modeling capability is especially valuable in complex projects because it supports a more accurate representation of how activities actually interact, rather than treating all dependencies as a single sequential pattern. PMI identifies PDM as a commonly used technique for developing project schedule network diagrams and recognizes these dependency relationship types. See the PMBOK® Guide and Standards and the PMI overview of precedence diagramming.

QUESTION NO: 5

Which of the following are NOT normally included in the project scope statement, either directly or by reference?

A. Project objectives in terms of cost, schedule and quality measures

B. Project contract between the contractor and owner

C. Project justification

D. Project deliverables

ANSWER: B

Explanation:

Project contract between the contractor and owner is correct because a project scope statement is principally a planning and control document that defines the work the project will deliver and the boundaries of that work. It establishes a common understanding of the required outcomes, including the project's deliverables, acceptance criteria, exclusions, assumptions, and constraints. In a physical-security project, it may describe such results as a completed access-control installation, camera coverage, integration requirements, testing, and acceptance activities. This definition enables the owner, security practitioner, designers, and implementation team to manage requirements and control scope changes throughout the project lifecycle.

By contrast, the contract is a distinct, legally enforceable procurement instrument between the owner and contractor. It governs the parties' legal relationship and may address commercial terms, payment, liability, insurance, dispute resolution, and contractual remedies, in addition to incorporating technical requirements. Although the scope statement can inform the statement of work and contract documents, the contract itself is not normally part of the project scope statement or a referenced scope-management component. PMI describes scope management as defining and controlling what is and is not included in a project: Project Scope Management. The U.S. General Services Administration likewise distinguishes a statement of work from the broader contractual structure in its acquisition guidance: GSA Acquisition Manual.

QUESTION NO: 6

Which information should be documented in an effective security incident report?

A. Observed facts

B. Actions taken by security personnel

C. Identity of witnesses when available

D. Speculation about a suspect's motive

ANSWER: A B C

Explanation:

Observed facts, **actions taken by security personnel**, and **the identity of witnesses when available** are correct. Incident reports should provide a clear, timely, factual record of what was observed, when and where it occurred, who was involved, the actions taken, notifications made, and any evidence preserved. Witness identification and contact information can support later investigation, provided information is collected and protected in accordance with policy and law. Reports should avoid unsupported conclusions, speculation, and inflammatory language because such statements can impair credibility and create unnecessary legal exposure. Accurate documentation supports management review, investigations, corrective action, and coordination with law enforcement. See the ASIS Standards and Guidelines.

QUESTION NO: 7

Which actions support continuity of operations after a physical-security incident disrupts a critical facility?

A. Identifying alternate operating locations

B. Maintaining current emergency contact information

C. Testing recovery procedures

D. Deferring identification of essential functions until after an incident

ANSWER: A B C

Explanation:

Identifying alternate operating locations, **maintaining current emergency contact information**, and **testing recovery procedures** are correct. Continuity planning addresses how an organization will sustain or restore priority functions when normal facilities, personnel, technology, or resources are disrupted. Alternate locations provide options when a primary site is unavailable; current contact information enables timely coordination; and exercises reveal gaps in procedures, communications, authority, and resource readiness before an actual incident occurs. Waiting until the incident is over to identify essential functions is inconsistent with continuity planning because those priorities should be established in advance. FEMA continuity guidance emphasizes planning, testing, training, and exercising to maintain essential functions. See FEMA Continuity of Operations.

QUESTION NO: 8

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 and **Threat response** are correct because electric-sector security guidance is built around identifying critical assets, evaluating threats and vulnerabilities, determining the resulting risk, and implementing measures to prevent, mitigate, and respond to security events. A vulnerability and risk analysis provides the structured basis for prioritizing protective resources: it considers the importance of an asset or facility, credible threat conditions, exploitable weaknesses, and the potential reliability or operational consequences of a successful attack. Threat response then turns that assessment into practical protective action, including response planning, coordination, recovery, and measures that reduce the likelihood or impact of an identified threat. These are complementary functions rather than separate alternatives: meaningful response measures should be informed by a documented risk assessment, while risk findings must lead to planned response and mitigation activities. This approach is reflected in NERC's mandatory physical-security framework. Reliability Standard CIP-014 requires applicable entities to identify critical facilities and conduct threat and vulnerability assessments, then develop and implement security plans to address identified risks. NERC's security standards also require documented incident-response planning and exercise activities for relevant cybersecurity incidents. See NERC Reliability Standards and NERC CIP-014-3, Physical Security.

QUESTION NO: 9

A good risk management program involves:

A. Identify risks or specific vulnerabilities

B. Analyze and study risks, including likelihood and degree of danger of an event

C. Study of security programs

D. All of the above

ANSWER: D

Explanation:

All of the above is correct because an effective risk management program is a structured, continuing process that incorporates each listed activity. It begins by identifying assets, threats, vulnerabilities, and the specific risk conditions that

could affect an organization. Identification provides the factual basis for deciding what requires protection and where resources should be focused. The program then analyzes those risks by considering the likelihood of an event or threat scenario and the magnitude of its potential consequences. This evaluation supports consistent prioritization and informs proportionate treatment decisions. Finally, studying security programs is necessary to determine whether current policies, procedures, personnel, technology, and physical safeguards adequately address the identified and analyzed risks. That review connects the assessment to practical security improvements and enables management to monitor effectiveness over time. Together, these activities reflect the core risk-management cycle of identifying, assessing, treating, and reviewing risk. ASIS security risk assessment guidance emphasizes a systematic process for evaluating risks and selecting appropriate protective measures, while NIST describes risk assessment as identifying threat sources and vulnerabilities and determining likelihood and impact. See ASIS Standards and Guidelines and NIST SP 800-30 Rev. 1.

QUESTION NO: 10

Project delays are best analyzed

A. After either the contractor or the owner acknowledges ^responsibility for the delay.

B. Contemporaneously with the delay.

C. By an expert after the project is finished when complete records are available and the impact is known.

D. Late in the project.

ANSWER: B

Explanation:

Contemporaneously with the delay. is correct because a delay analysis is most reliable when it is performed while the relevant work is occurring and project information is current. At that point, the project team can compare the planned schedule with actual progress, identify the specific activity or event causing the delay, preserve records, and evaluate effects on critical-path work before subsequent events obscure the causal relationship. Contemporaneous analysis also supports timely mitigation: the owner, contractor, and security project stakeholders can consider schedule recovery actions, resource adjustments, sequencing changes, notifications, or formal change-control decisions while those measures can still reduce operational and cost impacts.

For physical-security projects, where installation, integration, testing, commissioning, and site-access dependencies can affect one another, current documentation is especially important. Useful records include approved schedules and updates, daily reports, meeting minutes, change directives, delivery information, access restrictions, correspondence, and progress evidence. Maintaining and assessing these records as events unfold creates an auditable basis for managing the project and resolving responsibility fairly. This approach aligns with established construction delay guidance, which emphasizes contemporaneous records and proactive management of delay events. See the Society of Construction Law Delay and Disruption Protocol and the Project Management Institute's schedule-delay analysis guidance.

QUESTION NO: 11

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 is the correct selection because it is principally a business continuity, records-management, and disaster-recovery concern rather than an activity of crisis management itself. Vital-records planning identifies essential documents, data, and information assets; classifies their operational or legal importance; establishes retention requirements; and ensures that protected, recoverable copies are available after an interruption. This work supports the organization's ability to resume and sustain critical functions, but it is a preparedness and continuity capability that should be established and maintained before a crisis occurs.

A crisis management plan, by contrast, organizes leadership-level direction and coordination during a disruptive event: activating responsible personnel, making timely decisions, coordinating response operations, maintaining situational awareness, and managing communications with stakeholders and the public. Records protection can provide important information to those efforts, but the management, storage, backup, and restoration of vital records are normally addressed in continuity and recovery planning documentation. FEMA describes continuity planning as maintaining the capability to perform essential functions under all conditions, including planning for necessary resources and information. NIST likewise treats contingency planning as preparation for system recovery and restoration. See FEMA Continuity and NIST SP 800-34 Rev. 1.

QUESTION NO: 12

Which factors should be evaluated when selecting locations for exterior security lighting?

A. Potential concealment areas

B. Camera performance requirements

C. Glare affecting guards or drivers

D. Color of interior office furniture

ANSWER: A B C

Explanation:

Potential concealment areas, **camera performance requirements**, and **glare affecting guards or drivers** are correct. Exterior lighting should support observation and safe movement while limiting shadows and hiding places near entrances, parking areas, perimeter lines, and critical assets. Lighting design must also consider the needs of video surveillance because excessive contrast, glare, or poor illumination can degrade image quality. Improperly aimed luminaires can impair guards, vehicle operators, and neighboring occupants, creating both safety and operational problems. The color of interior office furniture is unrelated to exterior protective-lighting placement. See the U.S. Department of Energy outdoor lighting guidance and ASIS Standards and Guidelines.

QUESTION NO: 13

What defines a KPI?

A. Phase milestones

B. Initiation of a weather risk window

C. Key discrete project final or interim goals

D. Interim milestones related to weather phasing

E. A measurable value used to evaluate progress toward a defined objective

ANSWER: E

Explanation:

A measurable value used to evaluate progress toward a defined objective is the correct definition of a key performance indicator (KPI). In physical-security management, KPIs translate security objectives into quantifiable evidence that leaders can monitor, analyze, and use for decisions. For example, an organization seeking to improve access-control effectiveness

might track the percentage of access-control devices operational, the time taken to resolve alarm events, or the rate of credential-related policy exceptions. A useful KPI has a clearly defined purpose, a consistent calculation method, a data source, a target or threshold, an owner, and a defined review period. These elements allow performance to be compared over time and against the intended security outcome. KPIs can be used at strategic, operational, or project levels, but their defining feature is measurement of performance against an objective—not simply the existence of a date, deliverable, or event. This aligns with ISO management-system practice, which emphasizes monitoring, measurement, analysis, and evaluation of performance. See ISO 22301:2019—Business continuity management systems and APQC's definition and examples of KPIs.

QUESTION NO: 14

During a site survey, which conditions are indicators that natural surveillance may be inadequate?

A. Dense landscaping that obstructs views of doors and windows

B. Poorly illuminated pedestrian routes

C. A reception desk with a direct view of the main entrance

D. Concealed areas adjacent to parking facilities

E. Unobstructed sight lines between occupied work areas and exterior approaches

ANSWER: A B D

Explanation:

Dense landscaping that obstructs views, **poorly illuminated pedestrian routes**, and **concealed areas near entrances or parking facilities** are correct. Natural surveillance is a CPTED principle that seeks to provide legitimate occupants, security personnel, and passersby with clear opportunities to observe people and activity. Obstructed sight lines and inadequate lighting can provide opportunities for concealment and reduce the ability to detect suspicious behavior.

A building layout that allows reception personnel to observe an entrance supports natural surveillance rather than indicating a deficiency. Improvements may include vegetation maintenance, lighting upgrades, relocation of objects that create concealment, and positioning of legitimate activities to increase observation. See the CISA Physical Security resources.

QUESTION NO: 15

Is activity 7001 pictured correctly in the precedence diagram?

		Logic			Normal Schedule		Crashed Schedule	
ID	Activity	Succ.	Rel.	Lag	Days	Direct Costs	Days	Direct Costs
1000	General Conditions	11001	FF		1072	$3,080,000	910	$2,902,900
1001	Preliminary Civil Work	1000 2001 7001	SS FS FS		85	$563,000	67	$728,000
2001	River Diversion Stage 1	2002	FS		92	$150,000	75	$190,000
2002	River Diversion Stage 2	2003	FS		38	$25,000	28	35,000
2003	River Diversion Dam	2004 3001	FS FS		15	$18,000	11	$20,000
2004	River Diversion to Pipeline	3001 7001	FS FS		38	$96,000	38	$96,000
3001	Excavation, Dam Site	4001 4001 5001 5001 7001	SS FF SS FF FS	15 15 65 65	30	$482,000	100	$515,000
4001	Excavation, Spillway	5001 5001 9001	SS FF FS	45 45	152	$608,000	118	$692,000
5001	Drill and Grout Dam Site	6001	FS		102	$637,000	92	$650,000
6001	Rock Fill: to elevation 25	6002	FS		140	$1,352,000	105	$1,470,000
6002	Rock Fill: to elevation 38	6003	FS		115	$969,000	95	$1,125,000
6003	Rock Fill: to elevation 50	8001 9002 9002 9003	FS SS FF FS	65 65	152	$1,360,000	113	$1,540,000
7001	Permanent Roads	11001 9004	FS FS		48	$180,000	38	$205,000
8001	Valve House Embankment	9004	FS		28	$28,000	22	$36,000
9001	Spillway – Concrete	11001 9002 9003	FS FS FS		175	$1,120,000	155	$1,305,000
9002	Dam Concrete Facing – Concrete	1001 9005	FS FS		180	$1,260,000	160	$1,485,000
9003	Inlet Tower – Concrete 1 of 2	9005	FS	7	70	$275,000	65	$295,000
9004	Valve House – Concrete	10002	FS	7	72	$245,000	66	$265,000
	Inlet Tower –	10001	FS	7	35	$28,000	35	$28,000

9004	Valve House – Concrete	10002	FS	7	72	$245,000	66	$265,000

9005	Inlet Tower – Concrete 2 of 2	10001	FS	7	35	$28,000	35	$28,000
10001	Inlet Tower – Complete	11001	FS		25	$147,000	25	$147,000
	Valve House –	10001	FS		24	$132,000	24	$133,000

A. No, the total float is not shown correctly.

B. Yes, except the early finish date is not shown.

C. No, the start-to-start and finish-to-finish relationships are backwards.

D. Yes, the duration is 48 days.

ANSWER: D

Explanation:

Yes, the duration is 48 days. In a precedence diagram, an activity's duration is the planned working time required to complete that activity, independent of the relationship notation used to connect it with predecessor or successor activities. The activity information displayed for 7001 indicates a 48-day duration, so the activity is represented correctly in that respect. Precedence diagramming is the standard scheduling method for depicting project activities as nodes and connecting them through logical relationships; it supports calculation and display of schedule information such as early dates, late dates, and float. A correct review first confirms that the activity's own stated duration agrees with the schedule data shown for that node, then considers whether its linked relationships are consistent with the schedule logic. Here, the displayed duration for activity 7001 is 48 days, which supports the affirmative conclusion. This use of activity-on-node logic is consistent with the Project Management Institute's description of schedule-network diagramming and its guidance on developing and managing a project schedule. See the Project Management Institute's discussion of critical-path scheduling and the PMBOK Guide and Standards.

QUESTION NO: 16

Which of the following should be addressed in a security-system preventive-maintenance program?

A. Testing alarm devices and communications paths

B. Cleaning and inspecting cameras and housings

C. Verifying access-control door hardware operation

D. Deferring repairs until a system fails during an incident

E. Documenting deficiencies and corrective actions

ANSWER: A B C E

Explanation:

Testing alarm devices and communications paths, **cleaning and inspecting cameras and housings**, **verifying access-control door hardware operation**, and **documenting deficiencies and corrective actions** are correct. Preventive maintenance helps ensure that physical-security systems continue to perform as designed. Testing should verify not only that devices activate, but also that alarm signals are transmitted, received, displayed, assessed, and capable of initiating the intended response.

Deferring repair until a system fails is not preventive maintenance. Documentation supports accountability, trend analysis, warranty management, and confirmation that identified deficiencies were corrected. Maintenance requirements should follow manufacturer recommendations, organizational policy, and the site's risk-based performance requirements. See the CISA Physical Security resources.

QUESTION NO: 17

If all other work proceeds according to the Baseline plan, how many times will the critical path change?

Small Tower Crane

Typical capacity for a Small Crane

Maximum Load 5 tons

Minimum Load 1.5 tons

Operation	Time (in minutes)
Sling Up	5
Hoist Up	4
Discharge	3
Clear Unload Area	3
Hoist Down	2

A. 2.

B. 1.

C. Does not change.

D. 3.

ANSWER: C

Explanation:

Does not change. is correct because the critical path is the continuous sequence of dependent activities that determines the earliest possible project completion date. In the baseline network shown, proofing, printing, and packaging form that controlling sequence. If all other work continues in accordance with the baseline plan, no alternative sequence acquires a longer duration than this controlling sequence and no change occurs in the project's critical path. A critical path can change only when schedule performance or revised durations cause another path to become equally long or longer than the current controlling path. Maintaining the stated baseline performance for all remaining work preserves the established dependency logic, activity durations, and available float that support the original critical sequence. Accordingly, the project manager should continue monitoring the critical activities and their near-critical paths, but the stated condition does not produce a critical-path shift. This reflects the standard critical-path method principle that the path with zero or least total float controls the planned completion date. See the Project Management Institute's overview of critical-path scheduling and the PMI PMBOK® Guide and standards resources.

QUESTION NO: 18

When conducting a physical-security risk assessment, which of the following should be considered?

A. Threats

B. Vulnerabilities

C. Consequences

D. A guard's personal preference

ANSWER: A B C

Explanation:

Threats, **vulnerabilities**, and **consequences** are correct because risk assessment evaluates the relationship between a credible unwanted event, the weaknesses that may permit or worsen that event, and the effect that a successful event could have on the organization. Threat information helps define what may occur; vulnerability analysis identifies exploitable conditions; and consequence analysis establishes the potential impact on people, operations, assets, reputation, and

recovery. These findings enable security resources to be prioritized according to the organization's risk tolerance. A guard's personal preference is not a risk-assessment factor unless it is supported by relevant operational evidence. See NIST SP 800-30, Guide for Conducting Risk Assessments and ASIS Standards and Guidelines.

QUESTION NO: 19

Based on the available scope information and required accuracy, different cost estimated models or methodologies are utilized Which of the following statements is NOT true?

A. The Deterministic model is used when Class 3 through 1 estimates are required

B. The Parametric model is used when Class 5 or Class 4 estimates are required

C. The Deterministic model is used when Class 5 through 3 estimated are required

D. The Parametric model is used when detailed quantities are not known

ANSWER: C

Explanation:

The statement "The Deterministic model is used when Class 5 through 3 estimated are required" is not true because deterministic estimating requires a sufficiently defined scope and quantities that can be measured, priced, and assembled into a detailed estimate. That level of definition is generally associated with later estimate classes, particularly Class 3 through Class 1, rather than the earliest conceptual classes. Class 5 and Class 4 estimates are prepared when project definition is still limited; their purpose is to support screening, feasibility, or early decision-making rather than detailed cost development. At those early stages, estimating commonly relies on parametric relationships, capacity factors, historical benchmarks, and analogous-project data because detailed quantities are not yet available. The Association for the Advancement of Cost Engineering's estimate-class framework ties expected estimate accuracy and appropriate estimating methods to the maturity of project definition. As the scope becomes more complete, a deterministic, quantity-based build-up can replace the broader assumptions used for conceptual estimates. See AACE International Recommended Practices and the U.S. Government Accountability Office's Cost Estimating and Assessment Guide.

QUESTION NO: 20

What involves a discreet investigation into the past and present activities of the applicant?

A. Backgrounding

B. Reporting

C. Supervisory

D. Recording

ANSWER: A

Explanation:

Backgrounding is the discreet investigation of an applicant's past and current activities, identity, qualifications, character, and suitability for a position of trust. In a physical-security staffing context, it supports the organization's personnel-security objective: making an informed assessment of whether an individual may be granted access to facilities, assets, information, or sensitive duties. The scope is risk-based and commonly includes confirmation of identity, employment and education history, professional credentials, references, and—where lawful and relevant—criminal-history or other public-record checks. The investigation should be performed consistently, documented appropriately, limited to information relevant to the role, and handled confidentially. "Discreet" does not mean informal or unstructured; it means that the inquiry is conducted professionally, with proper authorization, respect for privacy, and controls over sensitive personal information. This aligns with recognized employment-screening practice, including obtaining appropriate disclosures and authorization when a third-party consumer reporting agency is used. The U.S. Equal Employment Opportunity Commission provides guidance on using arrest and conviction information in employment decisions at EEOC Enforcement Guidance. The Federal Trade Commission

also summarizes employer responsibilities for background reports under the Fair Credit Reporting Act at FTC: Background Screening.

QUESTION NO: 21 - (SIMULATION)

Background

Your name is Evan Marshal. You are the corporate scheduler for Happy Insurance Corporation (HIC), a general health insurance company located in Ridgemond, Illinois. HIC is very busy with 49 unique software development projects. The organization structure at HIC gives the project scheduling responsibility to the Project Manager assigned to each project. You are charged with coordination of the project schedules into a Master Schedule and quality control for scheduling on the individual development projects. You report directly to the Director of Information Services (DIS), Desmond Rayburn.

It has come to your attention Project JP-114 has fallen behind schedule and Rita Belateau, the Project Manager, wants to accelerate the project in order to reclaim lost time. Rita is a strong supporter of Total Quality Management and strives for zero failures; therefore she is assessing the need for overtime for resources assigned to an activity that is not projecting a completion prior to the early finish depicted in the current schedule.

You and Rita review the current schedule to identify which activities are on the critical path and which activities have plenty of float. The review reveals several activities have suffered less than planned productivity and have contributed to falling behind. In the process of this review, you and Rita also review the budget for Project JP-114 and notice not only the schedule has fallen behind but the cost to date is more than she had expected. To total budget is $150,000, planned to date is $30,000; expended to date is $37,000.

With nine months remaining until baseline contract completion, Rita needs to bring Project JP-114 back on track; knowing overtime for an extended period of time is not always the right answer, especially with the cost to date already over planned.

In order to truly understand the options available to help remedy the current situation, you and Rita brainstorm on several potential courses of action. All the potential courses of action will require an evaluation of budget impact versus schedule correction.

1. Pull the project team together and ensure everyone understands which activities are on the critical path. Rita would like to use the existing project team and focus them on these critical path activities, laying out a plan for periodic overtime when needed to crunch through a deliverable. This approach could add approximately 20% to the budget.

2. Outsource various modules of activities to qualified and known consultants. This could drive up the costs and must be evaluated before implemented. Having an outside source working in parallel with the project team could also accelerate the schedule to mitigate some of the delays, as well as keep overtime down to a minimum for the project team. Potentially this could add as much as 40% to the budget, but could also be very productive schedule wise.

3. Mandatory overtime for the project team - entire project goes on a 50-hour work week. If the entire project team works overtime for an extended period of time, the budget could see an additional 60% increase.

4. The project continues as is completes the project late and accepts the penalties imposed. Penalties imposed for late delivery could add as much as 50% to the budget.

Assignment

Draft a proper memorandum to Desmond Raybum, IS Director, explaining in your own words:

a. the current problem and potential impact(s);

b. each course of action, stating advantages and disadvantages as appropriate;

c. your recommendations, properly supported.

Please be sure to include the rationale for your recommendations. Be sure to summarize your thoughts and address (To, From, Date, and Subject/Project Name) and close the memo appropriately. If you are uncomfortable with the courses of action noted, provide your own with appropriate substantiation for your position. Limit your answer to one, full typewritten page (roughly three handwritten pages).

While your email can be a detailed as you like, be sure to write sufficiently to address each element of the assignment, yet not so long that you go beyond the scope of the exercise.

Take time to read the problem and consider what you want Evan to say. Good luck!

ANSWER: See the explanation for the answer

Explanation:

To: Desmond Rayburn, Director of Information Services
From: Evan Marshal, Corporate Scheduler
Date: [Current Date]
Subject: Project JP-114 Schedule-Recovery and Cost-Control Recommendation

Project JP-114 requires immediate corrective action. The project has spent $37,000 compared with $30,000 planned to date: a $7,000 variance, or 23.3% over the planned expenditure. Productivity below plan has delayed activities on the critical path. Unless the critical-path work is recovered, the project may miss its baseline contract completion date in nine months, incur delivery penalties, increase costs further, and affect customer confidence. Because the project is already over plan, any recovery action must be controlled against both schedule benefit and cost.

Options considered

Focus the existing team on critical-path activities and use limited, periodic overtime. This is the lowest-cost active recovery option, with a potential budget impact of approximately 20% (up to $30,000 against the $150,000 baseline). The team already understands the work and can begin quickly. The disadvantages are overtime cost, fatigue, and diminished productivity or quality if overtime becomes routine. Overtime on noncritical work would not recover the completion date and should not be authorized.
Outsource selected modules to known consultants. Parallel work can provide meaningful schedule compression and reduce internal overtime. However, the potential budget increase is up to 40% (up to $60,000), and consultant work creates risks of procurement delay, integration defects, communication overhead, and loss of control. Outsourcing work that is not on the critical or near-critical path may add cost without improving the finish date.
Require a mandatory 50-hour week for the entire project team. This may create short-term output, but it can increase the budget by as much as 60% (up to $90,000), and extended mandatory overtime raises fatigue, morale, turnover, quality, and rework risks. It also spends money on noncritical activities that do not shorten the project. I do not recommend this approach.
Continue as planned and accept late-delivery penalties. This avoids immediate disruption but does not correct the underlying problem. Penalties could add up to 50% (up to $75,000) to the budget, while a late delivery can damage HIC's reputation and stakeholder confidence. I do not recommend accepting this outcome without attempting recovery.

Recommendation

I recommend a controlled, phased combination of Options 1 and 2. First, revalidate the network schedule, remaining durations, logic, and resource assignments; identify the critical and near-critical paths; and establish a weekly schedule and cost recovery review. Direct the internal team to critical-path work and authorize only short, planned overtime for activities whose delayed completion would delay a critical-path successor. This targets the schedule problem while limiting the expected cost impact below the maximum 20% estimate.

Second, obtain a fixed-price or not-to-exceed proposal from qualified consultants only for discrete, separable modules on the critical or near-critical path, or for work that releases internal specialists to those paths. Each outsourcing decision should demonstrate more schedule gain than its added cost and include clear interfaces, acceptance criteria, quality reviews, and an integration owner. This selective use of consultants is preferable to committing immediately to the full 40% outsourcing exposure.

This approach avoids the unsustainable cost and quality risks of project-wide mandatory overtime and is more responsible than accepting penalties. It provides the best opportunity to meet the contractual date while protecting the remaining budget and maintaining TQM expectations. I will provide a revised critical-path schedule, recovery milestones, and forecast-at-completion after the schedule review and consultant estimates are complete.

Respectfully,
Evan Marshal
Corporate Scheduler

QUESTION NO: 22

: 20

Constraints control events or activities that _____.

A. Affect only the forward pass.

B. Are not based on project relationships.

C. Affect only the backward pass.

D. May be over-ridden by activity logic.

ANSWER: B

Explanation:

“Are not based on project relationships.” is correct because a schedule constraint is a date-based condition imposed on an activity or milestone, rather than a logical dependency derived from the network sequence. In a precedence network, relationships such as finish-to-start establish how one activity’s timing is calculated from another activity’s duration and timing. A constraint instead supplies an external scheduling requirement, such as requiring a milestone to occur on a specified date, preventing an activity from starting before a specified date, or requiring completion by a stated deadline. These requirements may arise from contractual commitments, regulatory deadlines, site-access windows, funding dates, or owner-directed delivery dates. Consequently, constraints are independent of the normal activity-to-activity relationships used to build the project network and calculate the schedule. They are important controls in physical-security project planning because equipment delivery, construction access, acceptance testing, and operational handover can be subject to fixed external dates. Scheduling references distinguish constraints from relationship logic and describe constraint types as restrictions on when an activity may start or finish. See Oracle Primavera’s activity constraint documentation and the Project Management Institute’s Project Management Lexicon for related scheduling terminology.

QUESTION NO: 23

Using th e crashed schedule, if you start Activity 2002 on 12 August 2021. what is the finish date for Activity 2002?

A. 19 Sep 2021

B. 08 Sep 2021

C. 09 Sep 2021

D. 27 Aug 2021

ANSWER: C

Explanation:

09 Sep 2021 is the correct finish date when Activity 2002 has the stated crashed duration of 28 days and begins on 12 August 2021. Schedule calculations normally apply the activity duration to its planned start according to the project calendar and the scheduling convention in use. On the calendar-day basis reflected by the available dates, adding 28 days to 12 August results in 09 September 2021. This is consistent with a crashed schedule because crashing reduces the planned duration of selected activities to achieve an earlier completion date; the resulting finish date must then be recalculated from the revised activity duration and start date. A reliable schedule also requires a defined calendar, since working-time calendars determine whether weekends, holidays, or other nonworking periods consume activity duration. In this question, the supplied crashed-duration calculation establishes 09 September 2021 as the intended completion date. ASIS PSP practitioners use schedule-development and schedule-control principles to assess how duration changes affect activity dates and the overall project timeline. For general scheduling terminology and calendar-based date calculation concepts, see the Project Management Institute PMBOK resources and the ASIS Physical Security Professional certification overview.

QUESTION NO: 24

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

E. Opportunity

ANSWER: E

Explanation:

Opportunity is the correct term. In loss-prevention practice, theft is most effectively reduced by identifying and controlling the conditions that make a loss possible or easy to commit. Those conditions can include unrestricted access to merchandise or assets, inadequate supervision, weak key and credential control, blind spots in surveillance coverage, poor inventory accountability, and ineffective receiving or cash-handling procedures. A loss prevention specialist may not be able to eliminate an offender's motivation or personal rationalization, but can directly influence the physical environment, procedures, and controls that create opportunity.

This approach is consistent with situational crime-prevention principles: practical security measures reduce crime by increasing the effort required, increasing the perceived risk of detection, and reducing access to attractive targets. A systematic assessment of opportunities therefore supports selecting proportionate controls such as access control, surveillance, inventory controls, employee training, and audit processes. These controls address the actionable component of the theft problem and are central to a risk-based physical-security program. See the ASIS Standards and Guidelines resources and the Center for Problem-Oriented Policing overview of situational crime prevention.

QUESTION NO: 25

Which statement is true?

A. Where compensability cannot be established, excusability is assumed.

B. Where compensability can be established, excusability cannot be assumed.

C. Where compensability cannot be established, excusability is a given.

D. Where compensability can be established, excusability is assumed.

ANSWER: D

Explanation:

"Where compensability can be established, excusability is assumed." is true because a compensable delay is a category of delay for which the owner is responsible and for which the contractor is entitled to both schedule relief and monetary recovery, subject to the contract's notice, documentation, and causation requirements. The entitlement to additional contract time means the delay is excusable: the contractor is not held responsible for failing to meet the affected completion date. The additional entitlement to recover delay-related costs is what makes the excusable delay compensable. In practical delay analysis, the security professional or project manager should distinguish the delay's cause, responsibility, effect on the critical path, and contractual remedy. Once the analysis establishes that an owner-caused action or omission created a compensable critical delay, the related excusable time extension follows as part of the remedy. This relationship supports fair allocation of schedule risk and helps ensure that the project record addresses both time and cost consequences. The Federal Acquisition Regulation similarly recognizes that certain causes beyond a contractor's control justify schedule relief, while clauses governing changes and equitable adjustments can establish monetary entitlement for government-responsible impacts. See FAR 52.249-10, Default (Fixed-Price Construction) and FAR 52.243-4, Changes.

QUESTION NO: 26

Which of the following practices support effective key-control management?

A. Maintaining an authorized key-holder record

B. Using a controlled key-issue and return process

C. Allowing employees to duplicate convenience keys as needed

D. Conducting periodic key inventories

E. Restricting access to master keys

ANSWER: A B D E

Explanation:

Maintaining an authorized key-holder record, **using a controlled key-issue and return process**, and **conducting periodic key inventories** are correct. Key control requires accountability throughout the key life cycle. The organization should identify who is authorized to receive each key, record issuance and return, protect master keys and key-cutting information, and reconcile keys through regular inventories or audits.

Keys should not be duplicated without approval because uncontrolled duplication defeats the accountability that the key-control program is intended to establish. When a key is lost, stolen, or not returned, the security manager should evaluate the affected access level and determine whether rekeying, cylinder replacement, or other corrective action is necessary. See the ASIS Standards and Guidelines resource center.

QUESTION NO: 27

Which provisions should be included in a contract for security-officer services to support measurable performance?

A. Defined post orders

B. Staffing and training requirements

C. Performance measures and reporting requirements

D. Authority for the provider to change post orders without client approval

E. Corrective-action procedures

ANSWER: A B C E

Explanation:

Defined post orders, **staffing and training requirements**, **performance measures and reporting requirements**, and **corrective-action procedures** are correct. A well-administered security-services contract establishes what the provider must deliver and how the client will evaluate performance. Post orders translate the security mission into site-specific duties, while staffing and training requirements establish the qualifications and readiness expected of assigned personnel.

Performance measures should be objective and relevant to the assignment, such as staffing fulfillment, patrol completion, report quality, training compliance, response performance, and supervisory inspections. Corrective-action procedures provide a documented process for addressing deficiencies. A provision allowing the provider to change post orders without client approval would undermine client control and accountability. See the ASIS Standards and Guidelines resource center.

QUESTION NO: 28

Which of the following are NOT considerations or constraints of the planning process for construction scheduling?

A. Consideration of all stakeholders.

B. Value engineering.

C. Project variables.

D. Interest rate of owner's construction bonds.

ANSWER: D

Explanation:

Interest rate of owner's construction bonds is the correct answer because it concerns the owner's financing cost rather than the planning logic used to develop and control a construction schedule. Construction scheduling establishes the sequence, duration, dependencies, resources, milestones, and constraints associated with physical project activities. Effective schedule planning also accounts for the needs of affected stakeholders, project-specific variables such as site conditions and available resources, and design or delivery decisions—such as value engineering—that can change work scope, methods, durations, or sequencing.

Although financing availability and payment timing may affect a project at a program-management level, the coupon or interest rate on the owner's bonds is not ordinarily a direct scheduling input. It does not define activity relationships, establish resource availability, or create a field-execution constraint. The distinction is important for physical-security projects because the security professional must coordinate construction work with operational requirements, phased occupancy, procurement lead times, and installation dependencies, while recognizing that bond-pricing decisions remain a financial matter. The U.S. General Services Administration describes scheduling as planning and tracking project work and milestones in its project-management guidance. The Construction Management Association of America also identifies scheduling as a core construction-management function in its construction-management overview.

QUESTION NO: 29

A good change management plan_____.

A. is provided to stakeholders after it is created

B. is detailed during the planning phase

C. tracks minor decisions

D. involves only the project controls team

ANSWER: B

Explanation:

is detailed during the planning phase is correct because effective change management must be designed before changes arise, not improvised after a project is underway. During planning, the security project team establishes the process for submitting a change request, documenting its purpose, assessing effects on scope, cost, schedule, risk, system performance, and security requirements, and identifying the authority that may approve or reject it. The plan should also define configuration documentation, version control, stakeholder communications, implementation steps, and verification that an approved change achieved its intended result without creating unacceptable vulnerabilities or operational impacts.

For physical security projects, this advance structure is especially important because a seemingly limited modification—such as altering a door schedule, camera coverage area, access-control rule, or installation sequence—can affect life safety, code compliance, procurement, integration, and the owner's operational needs. A documented process established in planning supports traceability and ensures that authorized stakeholders can make informed decisions throughout project execution. This aligns with project-management practice that treats change control as a planned, integrated governance process. See the Project Management Institute standards overview and ASIS's standards and guidelines resources.

QUESTION NO: 30

Which of the following is NOT the distinct action that fall into invasion of privacy?

A. misappropriation of the plaintiff's name or picture for commercial advantage

B. placing the plaintiff in the false light

C. private disclosure of public facts

D. intrusion into the seclusion of another

ANSWER: C

Explanation:

“private disclosure of public facts” is correct because it does not describe a recognized common-law privacy tort. The relevant distinct privacy action is *public disclosure of private facts*: publicity must be given to information that is genuinely private, and the disclosure must be highly offensive to a reasonable person. Reversing both concepts changes the meaning materially. Information that is already public generally lacks the private character required for this cause of action, while a disclosure made only privately ordinarily does not meet the publicity element. Thus, the stated phrase is not one of the established invasion-of-privacy actions.

The traditional privacy framework is commonly associated with the categories recognized in the Restatement (Second) of Torts: unreasonable intrusion upon seclusion, appropriation of name or likeness, unreasonable publicity concerning private life, and publicity that places a person in a false light. This classification is useful in physical-security practice because investigations, surveillance, records handling, and incident communications should be evaluated for possible privacy impacts under the applicable legal theory. See the Cornell Legal Information Institute overview of privacy and the Judicial discussion of the four privacy tort categories.

QUESTION NO: 31

The degree to which a manager or supervisor is able to delegate responsibility rather than trying to do everything personally is a good measure of managerial ability.

A. True

B. False

ANSWER: A

Explanation:

True is correct because effective delegation is a core managerial competency. A capable manager assigns appropriate responsibility and corresponding authority to qualified personnel, sets clear expectations, provides the resources and support needed to perform the work, and remains accountable for the outcome. This approach enables timely decisions, develops employees’ competence and confidence, improves continuity of operations, and allows the manager to focus attention on leadership, planning, risk management, and other responsibilities that cannot or should not be performed personally. In physical security operations, delegation is particularly important because supervisors must coordinate personnel, maintain coverage, respond to changing conditions, and ensure procedures are consistently carried out across shifts or locations. The ability to delegate appropriately therefore provides meaningful evidence of managerial ability: it reflects judgment about personnel capabilities, trust balanced with oversight, and effective use of organizational resources. Delegation does not mean abandoning accountability; rather, the manager retains responsibility for establishing controls, monitoring performance, and ensuring work supports organizational objectives. This principle is consistent with management guidance describing delegation as assigning responsibility and authority while the manager remains accountable. See Management Study Guide: Delegation and U.S. Office of Personnel Management.

QUESTION NO: 32

What involves walking or riding a given route to observe the condition of the facility?

A. Patrol duty

B. Posts

C. Reserves

D. None of the above

ANSWER: A

Explanation:

Patrol duty involves a security officer walking or riding a designated route to observe conditions throughout a facility. This activity provides a visible security presence while enabling the officer to identify such matters as unsecured doors, damaged barriers, unsafe conditions, equipment irregularities, fire or life-safety hazards, suspicious activity, and other deviations from normal operations. Patrols may be conducted on foot, by vehicle, bicycle, or other appropriate means, depending on the size, layout, risk profile, and operational requirements of the protected site.

Effective patrol duty is systematic rather than merely repetitive. Officers follow assigned routes and schedules while varying timing and patterns where appropriate, make observations using all available senses, check critical locations and access points, document findings accurately, and promptly report or respond to conditions requiring attention. The patrol function supports the core physical-security objectives of deterrence, detection, assessment, and response by ensuring that the facility's condition is actively monitored rather than assumed to be secure. ASIS guidance on security operations recognizes patrol as a fundamental protective-service activity within a comprehensive security program. See ASIS International's security officer training guidance and the ASIS Standards and Guidelines resource page.

QUESTION NO: 33

The characteristic of the precedence diagramming method that models construction projects differently than the arrow diagramming method is that it_____.

A. uses arrows to signify logic in a network

B. allows more than one critical path to be represented

C. can be used to calculate the late start and late finish of all activities

D. allows multiple relationship types to be associated with activities

ANSWER: D

Explanation:

The correct answer is "allows multiple relationship types to be associated with activities." The Precedence Diagramming Method (PDM), also called activity-on-node diagramming, represents activities as nodes and permits logical dependencies to be defined using finish-to-start, finish-to-finish, start-to-start, and start-to-finish relationships. It can also apply leads and lags to those relationships. This gives planners a more flexible way to model the actual sequencing and overlap of construction work, such as starting follow-on work once a predecessor has begun or requiring two activities to finish together. This is the key modeling characteristic that distinguishes PDM from the traditional Arrow Diagramming Method (ADM), which is generally associated with finish-to-start relationships and represents activities with arrows. In project scheduling, selecting a network-diagramming approach that accurately reflects work relationships is essential for calculating dates, identifying the critical path, and managing schedule changes. PMI describes PDM and its four dependency types in its scheduling guidance; see PMI's overview of the Precedence Diagramming Method. A concise explanation of the dependency relationship types is also available from ProjectManagement.com.

QUESTION NO: 34

Which measures can improve the effectiveness of a card-access control system?

A. Anti-passback controls

B. Timely removal of inactive credentials

C. Tailgating prevention procedures

D. Issuing visitor credentials without verification

ANSWER: A B C

Explanation:

Anti-passback controls, **timely removal of inactive credentials**, and **tailgating prevention procedures** are correct because each measure addresses a common weakness in access-control operations. Anti-passback can help prevent a credential from being passed back for repeated use. Prompt deactivation of credentials limits access by separated employees, expired contractors, and persons whose authorization has changed. Tailgating controls address the risk that an unauthorized person follows an authorized person through a controlled opening. Issuing one credential to every visitor without verification would weaken, rather than improve, access assurance. NIST guidance recognizes the importance of managing physical access authorizations and reviewing access rights. See NIST SP 800-53, Physical and Logical Access Controls.