

Physical Security Professional (PSP)

Examination Structure and Content

The PSP examination consists of multiple-choice questions covering tasks, knowledge and skills in subjects identified by physical security professionals as the major areas involved in this field. All exam questions come from the official reference books. No questions on the exam are taken from any other source.

The subjects are:

Physical Security Assessment [Approximately 41% of test questions]

A. Identifying assets to determine their value and criticality

- Nature and types of assets (e.g., property, personnel, and information)
- Valuing various types of assets
- Definitions and terminology
- Risk management principles
- Core functions of the facility
- Types of security programs and security processes
- Qualitative vs. quantitative risk assessments

B. Assessing the nature of the threats so that the scope of the problem can be determined.

- Nature, categories, and types of threats (e.g., natural, man-made)
- Nature of different types of environments (e.g., natural disasters, criminal events, terrorism)
- Crime demographics
- Critical business operations of various types of facilities
- External organizations and their potential impact on facility's security program

C. Conducting a physical security survey in order to identify the vulnerabilities of the organization.

- Security survey techniques
- Security technologies and equipment applications
- Interpretation of building plans, drawings and schematics
- Nature and types of data to be collected
- Methods of collecting relevant data
- Analysis and interpretation of relevant data
- Different levels of vulnerability and effects on assets

D. Performing a risk analysis so that appropriate countermeasures can be developed.

- Types of risk analyses
- Cost and loss analyses
- Methods of evaluating criticality and probability
- Appropriate countermeasures related to specific threats
- Legal issues related to various countermeasures/security applications

Selection of Integrated Physical Security Measures [Approximately 24% of test questions]

A. Identifying measures/components to match the requirements of the appropriate solution/recommendation

- Relevant terminology
- Types of security measures and their various applications (people and technology)
- Applicable codes and standards
- Appropriate hardware and software
- Ancillary measures
- Materials, equipment and system compatibility

B. Performing cost analysis of the proposed integrated measures to ensure efficiency of implementation/operation

- Types of security measures/equipment
- Cost estimates and cost-benefit analysis
- Integration of components/measures
- Scheduling

C. Outlining/documenting recommendations with relevant reasons for presentation to facility so that appropriate choices can be made

- Major elements of reports/proposals
- Methods of setting priorities
- Advantages and disadvantages of various security measures and management processes
- Drawings and plans

Implementation of Physical Security Measures [Approximately 35% of test questions]

A. Outlining criteria for pre-bid meetings to ensure comprehensiveness and appropriateness of implementations

- Bid package components
- Criteria for evaluation of bids
- Technical compliance criteria

B. Procuring systems and implementing recommended solutions to solve identified problems

- Project management functions and processes
- System integration
- Qualifying vendor factors
- Change order reviews
- Procurement process
- Passive and active designs

C. Conducting final acceptance testing and implementing/providing procedures for ongoing monitoring and evaluation of the measures

- Installation/maintenance inspection techniques
- Establishing test criteria
- End-user training requirements
- Maintenance needs of design
- Loss prevention techniques
- System programming techniques
- Asset tracking technologies
- Passive and active designs