PSP Body of Knowledge

To be awarded the PSP designation, a candidate must pass a comprehensive examination consisting of approximately 140 multiple-choice questions: 125 "live," scoreable questions and up to 15 pre-test questions. Knowledge in three major areas (domains) is tested.

importance of each domain, and the tasks, knowledge, and skills within it, determine the specifications of the PSP examination. The relative order of importance of the domains determines the percentage of total exam questions.

DOMAIN ONE

Physical Security Assessment (34%)

TASK 1: Develop a physical security assessment plan.

Knowledge of

1. Risk assessment models and considerations
2. Qualitative and quantitative assessment methods
3. Key areas of the facility or assets that may be involved in assessment
4. Types of resources needed for assessment

TASK 2: Identify assets to determine their value, criticality, and loss impact.

Knowledge of

1. Definitions and terminology related to assets, value, loss impact, and criticality
2. The nature and types of assets (tangible and intangible)
3. How to determine value of various types of assets and business operations

TASK 3: Assess the nature of the threats so that the scope of the problem can be determined.

Knowledge of

1. The nature, types, severity, and likelihood of threats and hazards (e.g., natural disasters, cyber, criminal events, terrorism, socio-political, cultural)
2. Operating environment (e.g., geography, socio-economic environment, criminal activity)
3. Potential impact of external organizations (e.g., competitors, supply chain, organizations in immediate proximity) on facility's security program
4. Other external factors (e.g., legal, loss of reputation, economic) and their impact on the facility's security program

TASK 4: Conduct an assessment to identify and quantify vulnerabilities of the organization.

Knowledge of

1. Relevant data and methods for collection (e.g., security survey, interviews, past incident reports, crime statistics, employee issues, issues experienced by other similar organizations)

2. Qualitative and quantitative methods for assessing vulnerabilities to probable threats and hazards
3. Existing equipment, physical security systems, personnel, and procedures
4. Effectiveness of security technologies and equipment currently in place
5. Interpretation of building plans, drawings, and schematics
6. Applicable standards/regulations/codes and where to find them
7. Environmental factors and conditions (e.g., facility location, architectural barriers, lighting, entrances) that impact physical security

TASK 5: Perform a risk analysis so that appropriate countermeasures can be developed.

Knowledge of

1. Risk analyses strategies and methods
2. Risk management principles
3. Methods for analysis and interpretation of collected data
4. Threat and vulnerability identification
5. Loss event profile analyses
6. Appropriate countermeasures related to specific threats
7. Cost benefit analysis (e.g., return on investment (ROI) analysis, total cost of ownership)
8. Legal issues related to various countermeasures/security applications (e.g., video surveillance, privacy issues, personally identifiable information)

DOMAIN TWO

Application, Design, and Integration of Physical Security Systems (34%)

TASK 1: Establish security program performance requirements.

Knowledge of

1. Design constraints (e.g., regulations, budget, cost, materials, equipment, and system compatibility)
2. Applicability of risk analysis results
3. Relevant security terminology and concepts
4. Applicable codes, standards and guidelines
5. Functional requirements (e.g., system capabilities, features, fault tolerance)
6. Performance requirements (e.g., technical capability, systems design capabilities)
7. Operational requirements (e.g., policies, procedures, staffing)
8. Success metrics

TASK 2: Determine appropriate physical security measures.

Knowledge of

1. Structural security measures (e.g., barriers, lighting, locks, blast migration, ballistic protection)
2. Crime prevention through environmental design (CPTED) concepts
3. Electronic security systems (e.g., access control, video surveillance, intrusion detection)
4. Security staffing (e.g., officers, technicians, management)
5. Personnel, package, and vehicle screening
6. Emergency notification systems
7. Principles of data storage and management
8. Principles of network infrastructure and network security

9. Security audio communications (e.g., radio, telephone, intercom, IP audio)
10. Systems monitoring and display (control centers/consoles)
11. Systems redundancy alternative power sources (e.g., battery, UPS, generators, surge protection)
12. Signal and data transmission methods
13. Considerations regarding Personally Identifiable Information (physical/logical/biometric)
14. Visitor management systems and circulation control

TASK 3: Design physical system and prepare construction and procurement documentation.

Knowledge of

1. Design phases (pre-design, schematic design, design development, construction documentation)
2. Design elements (calculations, drawings, specifications, review of manufacturer's submittals and technical data)
3. Construction specification standards (e.g., Construction specifications Institute, owner's equipment standards, American Institute of Architects MasterSpec)
4. Systems integration (technical approach, connecting with non-security systems)
5. Project management concepts
6. Scheduling (e.g., Gantt charts, PERT charts, milestones, and objectives)
7. Cost estimation and cost-benefit analysis of design options
8. Value engineering

DOMAIN THREE

Implementation of Physical Security Measures (32%)

TASK 1: Outline criteria for pre-bid meeting to ensure comprehensiveness and appropriateness of implementation.

Knowledge of

1. Bid package components
2. Criteria for evaluation of bids
3. Technical compliance criteria
4. Ethics in contracting

TASK 2: Procure system and implement recommended solutions to solve problems identified.

Knowledge of

1. Project management functions and processes throughout the system life cycle
2. Vendor pre-qualification (interviews and due diligence)
3. Procurement process

TASK 3: Conduct final acceptance testing and implement/provide procedures for ongoing monitoring and evaluation of the measures.

Knowledge of

1. Installation/maintenance inspection techniques
2. Systems integration
3. Commissioning
4. Installation problem resolution (punchlists)
5. Systems configuration management

6. Final acceptance testing criteria
7. End-user training requirements

TASK 4: Implement procedures for ongoing monitoring and evaluation throughout the system life cycle.

Knowledge of

1. Maintenance inspection techniques
2. Test and acceptance criteria
3. Warranty types
4. Ongoing maintenance, inspections and upgrade
5. Ongoing training requirements
6. Systems disposal and replacement processes

TASK 5: Develop requirements for personnel involved in support of the security program.

Knowledge of

1. Roles, responsibilities and limitations of security personnel (including proprietary (in-house) and contract security staff)
2. Human resource management
3. Security personnel training, development and certification
4. General, post and special orders
5. Security personnel uniforms and equipment
6. Personnel performance review and improvement processes
7. Methods to provide security awareness training and education for non-security personnel