PSP Body of Knowledge

To be awarded the PSP designation, a candidate must pass a comprehensive examination consisting of approximately 140 multiple-choice questions. The candidate will select one answer from the four choices offered. In total, there are 125 "live," scoreable questions and up to 15 pre-test questions. Knowledge in three major areas (domains) is tested.

The 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.

In 2022, ASIS conducted a job analysis study to ensure the PSP Body of Knowledge still represents the knowledge and skills needed to be a successful physical security manager. Only minor changes were made and noted below in green (these minor changes were made by the subject matter experts for better clarity). Exam questions regarding these updates will start to appear on the exam in late 2023.

DOMAIN ONE

Physical Security Assessment (34%)

Task 1: Develop a physical security assessment plan.

Knowledge of:

1. Key area or critical asset identification
2. Risk assessment models and considerations (e.g., inside-outward, outside-inward, site-specific risk assessment, functional approach)
3. Qualitative and quantitative assessment methods
4. Types of resources & guidelines needed for the assessment (e.g., stakeholders, budget, equipment, policies, standards)

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 for various types of assets and business operations

Task 3: Assess the nature of the threats and hazards so that the risk 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, socioeconomic environment, criminal activity, existing security countermeasures, security risk level)
3. Potential impact of external organizations (e.g., competitors, organizations in immediate proximity) on facility's security program
4. Other internal and external factors (e.g., legal, loss of reputation, economic, supply chain) 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, incident reports, crime statistics, personnel issues, issues experienced by other similar organizations)
2. Effectiveness of current security technologies/equipment, personnel, and procedures
3. Interpretation of building plans, drawings, and schematics
4. Applicable standards/regulations/codes and where to find them
5. Environmental factors and conditions (e.g., facility location, architectural barriers, lighting, entrances) that impact physical security]

Task 5: Perform a risk analysis to develop countermeasures.

Knowledge of:

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

DOMAIN TWO

Application, Design, and Integration of Physical Security Systems [35%]

Task 1: Establish security program performance requirements.

Knowledge of:

1. Design constraints (e.g., regulations, budget, materials, system compatibility)
2. Incorporation of risk analysis results in design
3. Relevant security terminology (e.g., punch list, field test)
4. Relevant security concepts (e.g., CPTED, defense-in-depth, the 4 Ds- deter, detect, delay, deny)
5. Applicable codes, standards, and guidelines
6. Operational requirements (e.g., policies, procedures, staffing)
7. Functional requirements (e.g., system capabilities, features, fault tolerance)
8. Performance requirements (e.g., technical capability, systems design capacities)
9. Success metrics

Task 2: Determine appropriate physical security countermeasures.

Knowledge of:

1. Structural security measures (e.g., barriers, lighting, locks, blast mitigation, ballistic protection)
2. Crime prevention through environmental design (CPTED)
3. Electronic security systems (e.g., access control, video surveillance, intrusion detection)
4. Security staffing (e.g., officers, technicians, management, administration)
5. Personnel, package, and vehicle screening
6. Emergency notification systems (e.g., mass notifications, public address, two-way intercom)
7. Principles of data storage and management (e.g., cloud, on-premise, redundancy, retention, user permissions, personally identifiable information, regulatory requirements)
8. Principles of network infrastructure and physical network security (e.g., token ring, LAN/WAN, VPN, DHCP vs. static, TCP/IP)
9. Security audio communications (e.g., radio, telephone, intercom, IP audio)
10. Systems monitoring and display (e.g., control centers/consoles, central monitoring station)
11. Primary and backup power sources (e.g., grid, battery, UPS, generators, alternative/renewable)
12. Signal and data transmission methods (e.g., copper, fiber, wireless)
13. Visitor and vendor management policies

Task 3: Design physical security systems and project documentation.

Knowledge of:

1. Design phases (e.g., pre-design, schematic development, construction, documentation)
2. Design elements (e.g., calculations, drawings, specifications, review, technical data)

3. Construction specification standards (e.g., Constructions Specifications Institute, Owner's equipment standards, American Institute of Architects (AIA) MasterSpec)
4. Systems integration
5. Project management concepts
6. Scheduling (e.g., Gantt charts, PERT charts, milestones, objectives)
7. Cost estimation and cost-benefit analysis of design options (e.g., value engineering)

DOMAIN THREE

Implementation of Physical Security Measures [31%]

Task 1: Outline criteria for pre-bid meeting.

Knowledge of:

1. Bid process (e.g., site visits, RFI, substitution requests, pre-bid meeting)
2. Bid package types (e.g., RFP, RFQ, IFB, sole source)
3. Bid package components (e.g., project timelines, costs, personnel, documentation, scope of work)
4. Criteria for evaluation of bids (e.g., cost, experience, scheduling, certification, resources)
5. Technical compliance criteria
6. Ethics in contracting

Task 2: Develop procurement plan for goods and services.

Knowledge of:

1. Vendor evaluation and selection (e.g., interviews, due diligence, reference checks)
2. Project management functions and processes
3. Procurement process

Task 3: Manage implementation of goods and services.

Knowledge of:

1. Installation and inspection techniques
2. Systems integrations
3. Commissioning
4. Installation problem resolution (e.g., punch lists)
5. Systems configuration management (e.g., as-built drawings)
6. Final acceptance testing criteria (e.g., system acceptance testing, factory acceptance testing)
7. End-user training requirements

Task 4: 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 (e.g., establishing KPIs, performance review, improvement processes, recruiting, onboarding, progressive discipline)
1. Security personnel professional development (e.g., training, certification)
2. General, post, and special orders
3. Security personnel uniforms and equipment
4. Security awareness training and education for non-security personnel

Task 5: Monitor and evaluate program throughout the system life cycle.

Knowledge of:

1. Maintenance of systems and hardware (e.g., preventative, corrective, upgrades, calibration, service agreements)
2. Warranty types (e.g., manufacturer, installation, replacement parts, extended)
3. Ongoing system training (e.g., system upgrades, manufacturer's certification)
4. System evaluation and replacement process