Course - Physical Security Professional (PSP) - ASIS

Duration – 5 Days

About the Course

The **Physical Security Professional (PSP)** preparation course provides in-depth knowledge required for professionals responsible for **physical security assessments, system design, and implementation of security countermeasures**.

The program develops competency in conducting **security surveys, threat analysis, risk assessment, physical security system design, procurement, and implementation of integrated protection systems**. Participants will gain the ability to design and implement **layered security strategies using people, processes, and technology**.

The course is aligned with the **PSP certification body of knowledge** and prepares candidates for the PSP certification examination.

Learning Outcomes

After completing this course, participants will be able to:

1. Conduct **physical security surveys and vulnerability assessments**.
2. Identify and evaluate **assets, threats, hazards, and vulnerabilities**.
3. Perform **risk analysis and cost-benefit analysis for security controls**.
4. Design **integrated physical protection systems**.
5. Select and integrate **security technologies and countermeasures**.
6. Manage **security system procurement, project design, and documentation**.
7. Implement and manage **physical security projects and systems**.
8. Evaluate **security system performance and maintenance requirements**.
9. Prepare effectively for the **PSP certification exam**.

Target Audience

This course is designed for:

- Physical security managers
- Security consultants
- Corporate security professionals
- Security system designers and engineers
- Facility security managers
- Risk and safety professionals
- Professionals preparing for the **PSP certification exam**

DAY 1– Physical Security Assessment (Part 1)

Module 1: Introduction to Physical Security

- Overview of physical security principles
- Layered security and defense-in-depth
- Role of physical security in risk management
- Security survey fundamentals

Module 2: Planning a Physical Security Assessment

- Developing assessment plans
- Scope definition and objectives
- Stakeholder identification
- Resources required for assessments

Module 3: Asset Identification and Criticality Analysis

- Identification of critical assets
- Asset classification (tangible and intangible)
- Determining asset value and loss impact
- Business process criticality

Module 4: Threat and Hazard Identification

- Types of threats (criminal, terrorism, insider threats)
- Natural hazards and environmental threats

- Sociopolitical and operational risks
- Threat likelihood and impact analysis

DAY 2 - Physical Security Assessment (Part 2)

Module 5: Vulnerability Assessment

- Methods for vulnerability identification
- Security surveys and inspections
- Facility walkthrough techniques
- Data collection methods

Module 6: Security Technology Evaluation

- Assessing current security technologies
- Evaluation of existing countermeasures
- Review of security procedures and personnel

Module 7: Facility and Environmental Analysis

- Building design considerations
- Architectural barriers
- Lighting and environmental factors
- Site layout and perimeter protection

Module 8: Risk Analysis and Countermeasure Development

- Risk analysis methodologies
- Threat-vulnerability-impact analysis
- Countermeasure identification
- Cost-benefit and ROI analysis

DAY 3 - Application, Design, and Integration of Physical Security Systems

Module 9: Principles of Security System Design

- Security design frameworks
- Crime Prevention Through Environmental Design (CPTED)
- Defense-in-depth strategy
- The **4Ds of security (Deter, Detect, Delay, Deny)**

Module 10: Physical Security Countermeasures

- Structural protection measures
- Locks and barriers
- Lighting systems
- Blast and ballistic protection

Module 11: Electronic Security Systems

- Access control systems
- Intrusion detection systems
- Video surveillance systems
- Alarm systems

Module 12: Security Communications and Monitoring

- Security communication systems
- Control rooms and monitoring centers
- Data transmission technologies
- Power systems and backup infrastructure

DAY 4 - System Design and Project Documentation

Module 13: System Integration

- Integration of security technologies
- Network infrastructure considerations
- System compatibility and interoperability

Module 14: Security Project Design

- Design phases (conceptual, schematic, detailed)
- Security drawings and specifications

- Technical documentation

Module 15: Security Project Management

- Project planning and scheduling
- Cost estimation and budgeting
- Risk considerations in design projects

Module 16: Vendor and Procurement Management

- Security procurement processes
- Vendor evaluation and selection
- Contract management

DAY 5 - Implementation of Physical Security Measures

Module 17: Security Project Implementation

- Implementation planning
- Installation processes
- Coordination with contractors and stakeholders

Module 18: Bid and Procurement Processes

- Request for Proposal (RFP)
- Request for Quotation (RFQ)
- Bid evaluation and contract awarding

Module 19: Testing and Commissioning

- System testing procedures
- Acceptance testing
- Commissioning of security systems

Module 20: Security Operations and Maintenance

- Monitoring and system management

- Preventive and corrective maintenance
- System performance evaluation