Associate Protection Professional (APP) - ASIS

Course Duration – 5 Days

About the Course

The **Associate Protection Professional (APP)** preparation course provides foundational knowledge required for professionals entering the security management field. The course focuses on the core competencies required to support organizational security programs, including **security fundamentals, business operations, risk management, and incident response**.

Participants will learn how security functions support organizational objectives, identify and manage risks, coordinate incident response, and implement effective security programs. The course prepares candidates for the **APP certification exam** and builds practical competence for real-world security environments.

Learning Outcomes

After completing the course, participants will be able to:

1. Explain the **principles of organizational security management**.
2. Support the **implementation of security programs and procedures**.
3. Conduct **basic risk identification and risk assessment activities**.
4. Understand **security investigations and evidence handling**.
5. Apply **business and operational principles in security management**.
6. Assist in **incident response, crisis management, and recovery activities**.
7. Demonstrate readiness for the **APP certification examination**.

Target Audience

This program is designed for:

- Entry-level **security professionals**
- Security officers and supervisors
- Corporate security team members
- Military or law-enforcement personnel transitioning to corporate security
- Risk, compliance, or safety professionals
- Individuals preparing for the **APP certification exam**

DAY 1 - Security Fundamentals (Part B)

Module 1: Introduction to Security Management

- Role of corporate security in organizations
- Security management concepts
- Organizational security governance
- Security policies and procedures

Module 2: Security Program Implementation

- Security program design and implementation
- Security planning and operational controls
- Security documentation and procedures
- Program monitoring and improvement

Module 3: Security Awareness Programs

- Developing security awareness programs
- Security training strategies
- Employee engagement in security
- Measuring awareness effectiveness

Module 4: External Security Relationships

- Liaison with law enforcement
- Coordination with government agencies
- Public–private security partnerships

DAY 2 - Security Fundamentals (Part B)

Module 5: Security Investigations

- Types of security investigations
- Investigation planning
- Interviewing and interrogation basics
- Investigative procedures

Module 6: Evidence and Documentation

- Evidence collection and preservation
- Chain of custody
- Documentation and reporting

Module 7: Personnel Security

- Background screening
- Pre-employment verification
- Employee security monitoring
- Ethics and privacy considerations

Module 8: Workplace Security Issues

- Workplace violence prevention
- Insider threats
- Executive protection basics

Module 9: Physical Security Concepts

- Access control systems
- Surveillance systems
- Physical barriers and protective technologies

DAY 3 - Business Operations

Module 10: Organizational Governance

- Organizational structures
- Corporate governance and compliance
- Role of security within business strategy

Module 11: Security Policies and Procedures

- Policy development and implementation
- Standard operating procedures
- Policy communication and enforcement

Module 12: Security Budgeting and Financial Management

- Budget planning for security programs
- Cost–benefit analysis
- Security investment justification

Module 13: Human Resource Management in Security

- Security staffing and workforce planning
- Training and development
- Performance management

Module 14: Vendor and Contract Management

- Vendor risk management
- Contract management for security services
- Outsourcing security operations

DAY 4 - Risk Management

Module 15: Fundamentals of Security Risk Management

- Risk concepts: threat, vulnerability, impact

- Enterprise Security Risk Management (ESRM)

Module 16: Risk Identification

- Threat identification
- Vulnerability analysis
- Security surveys and inspections

Module 17: Risk Assessment Methodologies

- Qualitative risk assessment
- Quantitative risk assessment
- Risk prioritization

Module 18: Risk Treatment and Mitigation

- Risk avoidance
- Risk reduction
- Risk transfer
- Risk acceptance

Module 19: Business Continuity Concepts

- Continuity planning
- Disaster recovery basics
- Resource planning for disruptions

DAY 5 - Response Management

Module 20: Incident Management Fundamentals

- Incident response lifecycle
- Incident classification
- Incident reporting

Module 21: Crisis and Emergency Management

- Crisis management planning
- Emergency preparedness
- Coordination with emergency services

Module 22: Incident Command Structure

- Incident command systems
- Emergency operations center (EOC)
- Roles and responsibilities during incidents

Module 23: Recovery and Post-Incident Activities

- Recovery planning
- After-action review
- Lessons learned and corrective actions

Module 24: APP Exam Preparation

- Domain review
- Sample exam questions
- Exam strategy and time management

Teaching Methodology

The course includes:

- Instructor-led lectures
- Case study discussion