# Course - Certified Protection Professional (CPP) - ASIS

## Duration – 5 Days

---

# About the Course

The **Certified Protection Professional (CPP)** preparation program develops advanced competencies required for professionals responsible for **enterprise security leadership and strategic security management**.

The course focuses on security governance, risk management, investigations, personnel security, physical protection systems, information security, and crisis management. Participants will learn how to design and manage enterprise security programs aligned with organizational objectives and risk management strategies.

The training is aligned with the **CPP body of knowledge** and prepares participants for the CPP certification examination.

---

# Learning Outcomes

After completing this course, participants will be able to:

1. Apply **security management principles and governance frameworks**.
2. Integrate **security strategy with business objectives**.
3. Conduct **security investigations and evidence handling**.
4. Implement **personnel security and insider threat programs**.
5. Design **physical security protection systems**.
6. Support **information security protection strategies**.
7. Plan and manage **crisis response and business continuity programs**.
8. Prepare effectively for the **CPP certification exam**.

---

KOENIG
step forward

# Target Audience

This course is intended for:

- Security managers and directors
- Corporate security leaders
- Risk and compliance managers
- Security consultants
- Law enforcement or military professionals transitioning to corporate security
- Professionals preparing for the **CPP certification exam**

---

# DAY 1 - Security Principles and Practices

## Module 1: Security Management Foundations

- Role of enterprise security management
- Security governance structures
- Security policies, procedures, and standards

## Module 2: Enterprise Security Risk Management (ESRM)

- Risk management concepts
- Threat, vulnerability, and impact analysis
- Security risk assessment frameworks

## Module 3: Security Program Development

- Designing enterprise security programs
- Security planning and implementation
- Security metrics and performance measurement

## Module 4: Legal and Regulatory Environment

- Legal considerations in security operations
- Compliance requirements
- Ethical responsibilities of security professionals

---

# DAY 2 - Business Principles and Investigations

## Module 5: Business Principles for Security Leaders

- Organizational governance
- Financial management and budgeting
- Security return on investment (ROI)

## Module 6: Project Management for Security Programs

- Security project lifecycle
- Resource planning and scheduling
- Vendor and contract management

## Module 7: Security Investigations

- Types of corporate investigations
- Investigation planning and procedures
- Evidence collection and preservation

## Module 8: Interviewing and Documentation

- Interview techniques
- Investigative documentation
- Reporting and legal considerations

---

# DAY 3 - Personnel Security

## Module 9: Personnel Security Programs

- Employee screening and vetting
- Background investigations
- Hiring and onboarding security processes

## Module 10: Insider Threat Management

- Insider threat identification
- Behavioral indicators
- Prevention and mitigation strategies

## Module 11: Workplace Violence Prevention

- Risk factors and warning signs
- Prevention strategies
- Incident response planning

## Module 12: Security Awareness and Training

- Employee awareness programs
- Security culture development
- Training program evaluation

---

# DAY 4 - Physical Security and Information Security

## Module 13: Physical Security Program Design

- Defense-in-depth strategy
- Layered security models
- Crime Prevention Through Environmental Design (CPTED)

## Module 14: Physical Security Systems

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

## Module 15: Information Security Fundamentals

- Information asset protection
- Cybersecurity risks and threats
- Data protection strategies

## Module 16: Integration of Physical and Information Security

- Converged security models
- Technology integration
- Security operations centers

---

# DAY 5 - Crisis Management

## Module 17: Crisis and Emergency Management

- Crisis management frameworks
- Emergency preparedness
- Incident command structures

## Module 18: Business Continuity Management

- Business impact analysis
- Continuity planning
- Disaster recovery strategies

## Module 19: Incident Response and Recovery

- Incident response coordination
- Crisis communication
- Recovery planning and restoration

KOENIG
step forward

# Module 20: Post-Incident Review

- Lessons learned
- Continuous improvement
- Updating crisis management plans

---