Security Management Professional (SMP) Certification Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Security Management Professional (SMP) Certification Training Course equips participants with advanced knowledge, strategies, and practical tools to design, implement, and manage comprehensive security programs across diverse organizational settings. The course focuses on emerging threats, risk mitigation strategies, crisis management, and the integration of physical, digital, and personnel security measures. Participants gain expertise in security policy development, compliance frameworks, investigative techniques, and modern security technologies, enabling them to safeguard assets, information, and personnel effectively.

In an era marked by increasing cybersecurity threats, global terrorism, insider risks, and complex regulatory demands, organizations require security professionals who can proactively anticipate, assess, and mitigate potential risks. This course combines theoretical knowledge with real-world case studies and practical exercises, ensuring participants are equipped to lead security operations, respond to incidents, enforce compliance, and develop strategic security initiatives that align with organizational objectives. The curriculum emphasizes operational resilience, situational awareness, and leadership in security management to foster a proactive and adaptive security culture.

Programme Curriculum

Security Management Professional (SMP) Certification Training Course

Introduction

Security Management Professional (SMP) Certification Training Course equips participants with advanced knowledge, strategies, and practical tools to design, implement, and manage comprehensive security programs across diverse organizational settings. The course focuses on emerging threats, risk mitigation strategies, crisis management, and the integration of physical, digital, and personnel security measures. Participants gain

expertise in security policy development, compliance frameworks, investigative techniques, and modern security technologies, enabling them to safeguard assets, information, and personnel effectively.

In an era marked by increasing cybersecurity threats, global terrorism, insider risks, and complex regulatory demands, organizations require security professionals who can proactively anticipate, assess, and mitigate potential risks. This course combines theoretical knowledge with real-world case studies and practical exercises, ensuring participants are equipped to lead security operations, respond to incidents, enforce compliance, and develop strategic security initiatives that align with organizational objectives. The curriculum emphasizes operational resilience, situational awareness, and leadership in security management to foster a proactive and adaptive security culture.

Course Objectives

1. Understand the fundamentals of security management and professional standards.
2. Identify and assess organizational risks across physical, digital, and personnel domains.
3. Develop comprehensive security policies, protocols, and compliance frameworks.
4. Apply risk assessment and mitigation strategies for diverse operational environments.
5. Implement advanced surveillance, access control, and monitoring systems.
6. Manage crisis and emergency response plans effectively.
7. Conduct investigations and intelligence gathering to prevent security breaches.
8. Integrate cybersecurity principles into physical and organizational security.
9. Develop business continuity and disaster recovery strategies.
10. Strengthen leadership and decision-making in security management roles.
11. Apply legal, ethical, and regulatory compliance standards in security operations.
12. Utilize technology and analytics for threat detection and security optimization.
13. Promote organizational security culture and employee awareness programs.

Organizational Benefits

- Enhanced organizational resilience against threats and vulnerabilities
- Improved risk assessment and mitigation capabilities
- Strengthened security governance and compliance adherence
- Reduced financial and reputational losses due to security incidents
- Increased operational efficiency through proactive threat management
- Enhanced situational awareness and incident response readiness
- Integration of physical and digital security measures
- Improved employee awareness and security culture
- Advanced use of technology in monitoring and security operations
- Competitive advantage through certified security leadership

Target Audiences

- Security managers and officers
- Risk management professionals
- Corporate compliance and audit teams
- IT and cybersecurity managers
- Facility and operations managers
- Law enforcement liaison officers
- Private security consultants
- Executive leadership involved in security strategy

Course Duration: 10 days

Course Modules

Module 1: Introduction to Security Management

- Principles of security management and organizational objectives
- Roles and responsibilities of security professionals
- Security standards, regulations, and certifications
- Risk-based security planning and policy frameworks
- Emerging trends in global security challenges
- Case Study: Security framework implementation in a multinational corporation

Module 2: Risk Assessment and Threat Analysis

- Identifying physical, digital, and operational risks
- Conducting vulnerability assessments and audits
- Threat modeling and scenario planning
- Prioritization of risk mitigation strategies
- Continuous monitoring and risk reporting
- Case Study: Threat assessment in a corporate headquarters

Module 3: Security Policy and Governance

- Designing comprehensive security policies and procedures
- Implementing governance frameworks for compliance
- Regulatory requirements and industry standards
- Documentation and reporting mechanisms
- Policy enforcement and review cycles
- Case Study: Policy redesign after a major security breach

Module 4: Physical Security Management

- Access control systems and surveillance technologies
- Perimeter security and facility protection measures
- Security personnel management and training
- Emergency preparedness and response drills
- Integration of physical and electronic security controls
- Case Study: Enhancing campus security in a corporate setting

Module 5: Cybersecurity Integration

- Cybersecurity fundamentals for security professionals
- Threat detection, monitoring, and incident response
- Network security controls and encryption strategies
- Managing insider threats and data breaches
- Cybersecurity compliance and audits
- Case Study: Cybersecurity breach mitigation in an MFI

Module 6: Crisis and Emergency Management

- Crisis response planning and command structures

- Business continuity and disaster recovery planning
- Communication strategies during emergencies
- Coordination with emergency services and stakeholders
- Post-crisis analysis and lessons learned
- Case Study: Crisis response during an industrial incident

Module 7: Investigations and Intelligence

- Principles of internal and external investigations
- Evidence collection, documentation, and chain of custody
- Interviewing techniques and investigative procedures
- Intelligence gathering and risk forecasting
- Legal and ethical considerations in investigations
- Case Study: Fraud detection and investigation in a corporate environment

Module 8: Security Technology and Surveillance

- Modern security technologies for monitoring and detection
- CCTV, sensors, and access control systems
- Integration of IoT and smart building technologies
- Analytics and reporting for operational insights
- Technology selection and vendor evaluation
- Case Study: Deployment of integrated surveillance systems

Module 9: Human Resource Security and Training

- Security awareness programs for employees
- Insider threat management and monitoring
- Background checks and vetting procedures
- Security culture development strategies
- Staff training and performance monitoring
- Case Study: Developing a corporate security awareness program

Module 10: Legal and Regulatory Compliance

- Security-related legal frameworks and obligations
- Industry standards and professional ethics
- Compliance auditing and reporting
- Handling legal liabilities and incident documentation
- Cross-border regulations and multinational compliance
- Case Study: Navigating regulatory compliance during global expansion

Module 11: Business Continuity Management

- Identifying critical business functions and dependencies
- Continuity planning and disaster recovery strategies
- Redundancy and backup systems
- Testing and simulation exercises
- Review and continuous improvement processes
- Case Study: Implementing continuity plans after a natural disaster

Module 12: Risk Communication and Reporting

- Internal and external reporting structures
- Communicating risk to management and stakeholders
- Crisis communication plans
- Reporting tools, dashboards, and KPIs
- Feedback loops for continuous security improvement
- Case Study: Communicating risk during a security incident

Module 13: Security Leadership and Decision-Making

- Strategic decision-making frameworks in security management
- Leading security teams effectively
- Coordination across departments and external partners
- Resource allocation and prioritization
- Ethical and professional leadership in high-risk environments
- Case Study: Leadership during a coordinated security response

Module 14: Emerging Threats and Global Security Trends

- Terrorism, cybercrime, and organized crime trends
- Threats in critical infrastructure and urban environments
- Monitoring geopolitical risks for organizational security
- Preparing for new and evolving security challenges
- Proactive and adaptive security planning
- Case Study: Responding to evolving cyber and physical threats

Module 15: Security Program Evaluation and Continuous Improvement

- Key performance indicators for security programs
- Conducting internal and external audits
- Continuous improvement and policy updates
- Benchmarking against industry standards
- Lessons learned and best practices for sustainability
- Case Study: Evaluating and enhancing an existing corporate security program

Training Methodology

- Instructor-led presentations and interactive discussions
- Hands-on exercises and simulation scenarios
- Group case study analysis and problem-solving workshops
- Technology demonstrations and practical applications
- Peer learning and role-playing exercises
- Action plan creation and facilitator feedback sessions

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com