Physical Security Design and Risk Assessment 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

Physical security design and risk assessment are critical components of organizational resilience, safeguarding assets, personnel, and information from potential threats. Modern threats, ranging from burglary and vandalism to terrorism and insider risks, demand a strategic approach that combines architectural planning, technology deployment, and operational protocols. Physical Security Design and Risk Assessment Training Course provides participants with comprehensive knowledge and practical frameworks for designing secure facilities, assessing vulnerabilities, and implementing multi-layered protection measures. Participants will also explore risk modeling, security audits, and compliance with industry standards to enhance the overall safety posture of organizations.

The course emphasizes practical application through scenario-based exercises, case studies, and hands-on design planning. Participants will gain insights into threat identification, access control systems, surveillance strategies, perimeter security, emergency response planning, and risk mitigation techniques. By the end of the training, learners will be equipped to develop, implement, and monitor physical security strategies that protect people, property, and information assets, ensuring organizational resilience and operational continuity.

Programme Curriculum

Physical Security Design and Risk Assessment Training Course

Introduction

Physical security design and risk assessment are critical components of organizational resilience, safeguarding assets, personnel, and information from potential threats. Modern threats, ranging from burglary and vandalism to terrorism and insider risks, demand a strategic approach that combines architectural planning, technology deployment, and operational protocols. Physical Security Design and Risk Assessment Training Course

provides participants with comprehensive knowledge and practical frameworks for designing secure facilities, assessing vulnerabilities, and implementing multi-layered protection measures. Participants will also explore risk modeling, security audits, and compliance with industry standards to enhance the overall safety posture of organizations.

The course emphasizes practical application through scenario-based exercises, case studies, and hands-on design planning. Participants will gain insights into threat identification, access control systems, surveillance strategies, perimeter security, emergency response planning, and risk mitigation techniques. By the end of the training, learners will be equipped to develop, implement, and monitor physical security strategies that protect people, property, and information assets, ensuring organizational resilience and operational continuity.

Course Objectives

1. Understand principles of physical security design and risk management frameworks.
2. Identify threats, vulnerabilities, and potential impact on organizational assets.
3. Conduct comprehensive risk assessments for facilities and operational sites.
4. Design multi-layered security systems integrating technology and human elements.
5. Apply access control measures and surveillance solutions effectively.
6. Implement perimeter protection, barriers, and intrusion detection systems.
7. Develop emergency response and contingency plans for diverse scenarios.
8. Integrate physical security with cyber and information security practices.
9. Evaluate compliance with industry standards and regulatory requirements.
10. Use threat modeling and scenario analysis to prioritize security investments.
11. Conduct security audits, gap analysis, and performance evaluations.
12. Train and manage security personnel for effective operational readiness.
13. Establish monitoring, reporting, and continuous improvement processes.

Organizational Benefits

- Strengthened protection of personnel, assets, and critical infrastructure
- Reduced risk of loss, theft, and operational disruption
- Enhanced compliance with safety and security regulations
- Improved emergency preparedness and response capabilities
- Increased resilience against internal and external threats
- Optimized allocation of security resources and budgets
- Greater confidence among stakeholders and clients
- Enhanced situational awareness and threat detection
- Better integration of security systems and processes
- Stronger organizational reputation for safety and reliability

Target Audiences

- Security managers and facility officers
- Risk management and compliance professionals
- Safety and emergency response coordinators
- Operations and logistics managers
- Security consultants and auditors
- Government and corporate security personnel
- IT and cybersecurity integration teams
- Architects and facility planners

Course Duration: 10 days

Course Modules

Module 1: Fundamentals of Physical Security

- Principles of physical security design
- Threat and vulnerability overview
- Security planning and policy frameworks
- Security layers and integrated approaches
- Security standards and regulations
- Case Study: Designing a secure office facility

Module 2: Threat Identification & Risk Assessment

- Threat modeling and classification
- Identifying vulnerabilities in physical infrastructure
- Risk assessment methodologies and tools
- Prioritizing risks based on likelihood and impact
- Evaluating historical incident data
- Case Study: Risk assessment of a financial institution

Module 3: Perimeter Security & Access Control

- Fencing, gates, and barrier systems
- Physical entry controls and authentication methods
- Visitor management systems
- Security signage and demarcation
- Integration with electronic access controls
- Case Study: Multi-layered perimeter security in a corporate campus

Module 4: Surveillance & Monitoring Systems

- CCTV design and deployment
- Alarm systems and sensors
- Remote monitoring and control centers
- Integrating video analytics for threat detection
- Maintenance and reliability considerations
- Case Study: Surveillance upgrade for a logistics hub

Module 5: Intrusion Detection & Alarm Systems

- Types of intrusion detection systems
- Sensor technologies and placement
- Alarm response protocols
- False alarm reduction strategies
- Integrating IDS with access control
- Case Study: Implementing intrusion detection in a manufacturing plant

Module 6: Security Lighting & Environmental Design

- Principles of effective security lighting

- Crime Prevention Through Environmental Design (CPTED)
- Landscaping and natural barriers
- Lighting audits and optimization
- Maintenance and energy considerations
- Case Study: CPTED application in a commercial complex

Module 7: Emergency Response & Contingency Planning

- Emergency planning frameworks
- Evacuation and lockdown procedures
- Crisis communication strategies
- Coordination with local authorities
- Testing and drills for preparedness
- Case Study: Emergency response plan for a hospital

Module 8: Security Personnel Management

- Recruitment, training, and supervision of security staff
- Roles and responsibilities of personnel
- Patrol and monitoring techniques
- Performance evaluation and accountability
- Integration with technology systems
- Case Study: Enhancing personnel readiness in a university campus

Module 9: Cyber-Physical Security Integration

- Linking physical and information security
- Threats from IoT and connected devices
- Secure data handling in security operations
- Incident detection and cross-domain response
- Policy and governance for integrated security
- Case Study: Cyber-physical security in a data center

Module 10: Risk Mitigation Strategies

- Prioritizing mitigation measures
- Cost-benefit analysis of security solutions
- Redundancy and failover planning
- Insurance and liability considerations
- Continuous risk monitoring
- Case Study: Risk mitigation in a retail chain

Module 11: Security Audits & Compliance

- Audit planning and execution
- Gap analysis and reporting
- Corrective action implementation
- Compliance with international and local standards
- Continuous improvement cycles
- Case Study: Security audit of a corporate campus

Module 12: Security Policies & Governance

- Developing institutional security policies
- Governance frameworks for decision-making
- Roles of committees and leadership
- Documentation and reporting practices
- Stakeholder communication and approvals
- Case Study: Policy overhaul in a financial institution

Module 13: Transportation & Mobile Security

- Vehicle fleet protection strategies
- Secure transport of cash and assets
- GPS tracking and route risk analysis
- Driver and personnel protocols
- Incident response for mobile operations
- Case Study: Safe cash transport in a bank network

Module 14: High-Risk & Critical Infrastructure Protection

- Identifying high-value targets
- Security planning for critical facilities
- Threat intelligence and scenario analysis
- Redundancy and emergency response measures
- Collaboration with authorities and agencies
- Case Study: Critical infrastructure protection plan for an energy plant

Module 15: Security System Testing & Continuous Improvement

- Testing and evaluation of security systems
- Performance metrics and KPIs
- Lessons learned from incidents and audits
- Updating protocols and infrastructure based on feedback
- Staff retraining and drills
- Case Study: Continuous improvement in a manufacturing facility

Training Methodology

- Instructor-led presentations and expert-led discussions
- Practical workshops on risk assessment and security design
- Hands-on exercises in access control and surveillance planning
- Scenario-based simulations for emergency response
- Case study analysis and group problem-solving activities
- Development of actionable security improvement plans

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