SKILLSLAB
Training Provider

COURSE BROCHURE

# Security Risk Management

Professional Training Course

Skillslab Training Provider
Skills for Tomorrow's World

info@skillslab-training.com | +966 55 965 3447 | www.skillslab-training.com

# Course Description

## Introduction

Security Risk Management is a premium professional training program designed for government entities, ministries, public sector organizations, large corporations, critical infrastructure operators, and executive professionals responsible for protecting people, assets, facilities, information, operations, and institutional reputation. In today's complex threat environment, organizations face evolving security risks including physical security breaches, workplace violence, insider threats, fraud-related exposure, supply chain disruption, civil unrest, terrorism-related threats, cyber-physical vulnerabilities, and crisis situations that can severely affect operational continuity and public confidence. This course provides a strategic and practical learning experience focused on security risk assessment, threat identification, vulnerability analysis, security planning, protective measures, incident response, crisis coordination, and organizational resilience. The executive-level value of this program lies in helping organizations move from reactive security practices to a structured, intelligence-led, and risk-based security management approach that supports safer operations, stronger governance, regulatory alignment, and sustainable institutional protection.

## Course Objectives

- Develop a strong understanding of security risk management principles, threat assessment, vulnerability analysis, and protective security planning.
- Strengthen the ability to identify internal and external security threats affecting people, assets, facilities, operations, and reputation.
- Apply practical security risk assessment methods for corporate, government, public sector, industrial, and critical infrastructure environments.
- Improve security planning, incident prevention, access control, emergency coordination, and response readiness.
- Understand how to design proportionate security controls based on risk level, operational context, and business priorities.

- Develop practical improvement plans to strengthen security posture and reduce exposure to disruptive threats.

## Course Content

### Day 1: Foundations of Security Risk Management

- Understanding the strategic importance of security risk management in modern organizations.
- Key concepts: security risk, threat, vulnerability, exposure, consequence, likelihood, control effectiveness, and residual risk.
- Security risks affecting government entities, public institutions, corporations, industrial sites, commercial facilities, and critical infrastructure.
- The relationship between security, governance, operational continuity, public trust, and institutional reputation.
- The role of leadership in building a proactive and risk-based security culture.
- Understanding physical security, personnel security, information-related security, operational security, and crisis readiness.
- Legal, regulatory, governance, and organizational expectations for security risk management.
- Common weaknesses in security programs and lessons learned from major security incidents.

### Day 2: Threat Identification, Vulnerability Assessment, and Risk Analysis

- Identifying internal and external threats across different organizational environments.
- Assessing threats related to unauthorized access, workplace violence, theft, sabotage, civil disturbance, insider activity, terrorism-related risks, and third-party exposure.
- Conducting vulnerability assessments for facilities, operations, systems, processes, and people.
- Evaluating likelihood, impact, exposure, attractiveness, capability, intent, and control gaps.
- Developing security risk registers and prioritizing risks based on severity and operational significance.
- Mapping critical assets, sensitive areas, high-risk functions, and essential services.
- Integrating security risk assessment with enterprise risk management and operational planning.
- Practical workshop: conducting a security risk assessment for an organizational scenario.

### Day 3: Security Controls, Protective Measures, and Operational Security

culture.

- Managing security risks in receptions, control rooms, storage areas, executive offices, public-facing facilities, and restricted zones.
- Security procedures for events, travel, VIP visits, high-profile meetings, and sensitive operations.
- Contractor and supplier security management in complex operational environments.
- Balancing security effectiveness with operational efficiency, user experience, and organizational culture.
- Practical exercise: developing a layered security control plan.

### Day 4: Incident Response, Crisis Coordination, and Security Communication

- Preparing for security incidents and disruptive events.
- Security incident response procedures, escalation paths, notification protocols, and decision-making authority.
- Coordinating with law enforcement, emergency services, regulators, internal departments, contractors, and external stakeholders.
- Managing incidents involving unauthorized entry, suspicious activity, workplace threats, protest activity, theft, sabotage, and facility disruption.
- Crisis communication during security-related incidents.
- Protecting evidence, documenting incidents, and supporting post-incident investigation.
- Linking security response with emergency response, business continuity, and crisis management plans.
- Simulation exercise: managing a security incident and coordinating organizational response.

### Day 5: Security Governance, Performance Improvement, and Implementation Roadmap

- Building a security governance framework aligned with organizational strategy and risk appetite.
- Roles and responsibilities of leadership, security teams, operations, human resources, legal, compliance, facilities, and communications.
- Security policies, procedures, standards, audits, inspections, reporting, and management review.
- Security performance indicators, incident trends, control testing, and continuous improvement.
- Training, awareness, drills, scenario planning, and security culture development.
- Learning from incidents, near misses, audit findings, and emerging threat intelligence.
- Developing a security risk management improvement roadmap.
- Final applied activity: presenting a practical security risk management plan for an organizational environment.

- Government officials, ministry representatives, regulators, and public sector professionals involved in institutional security and risk oversight.
- Security managers, security supervisors, physical security professionals, and protective services teams.
- Risk management, compliance, internal audit, business continuity, and crisis management professionals.
- Facility managers, operations managers, administration managers, and site leaders.
- Human resources, legal, corporate communication, and public relations professionals involved in security-related response.
- Project managers, contractor management teams, event managers, and critical infrastructure professionals.
- Professionals responsible for protecting people, assets, information, facilities, public trust, and operational continuity.

## Course Requirements

- Basic awareness of organizational operations, security practices, risk management, or facility management is helpful.
- No advanced technical or specialist security background is required.
- Participants are encouraged to bring examples of security procedures, incident reports, facility risks, access control challenges, or security improvement priorities from their organizations.
- The course is suitable for both experienced professionals and managers newly assigned to security risk management responsibilities.

## Training Methodology

- Executive-level presentations supported by practical security risk management examples.
- Interactive discussions focused on real threats facing government, public sector, corporate, industrial, and critical infrastructure environments.
- Case-based learning on security incidents, access control failures, insider threats, and crisis coordination challenges.
- Practical exercises in threat identification, vulnerability assessment, security control design, and incident response.
- Group workshops for developing security risk registers, protective measures, and implementation roadmaps.
- Scenario-based simulations to strengthen decision-making during security incidents and disruptive events.

By the end of this Security Risk Management training course, participants will be able to:

- Explain the principles of security risk management, threat assessment, vulnerability analysis, and protective security planning.
- Identify key security threats and vulnerabilities affecting people, assets, facilities, operations, and reputation.
- Conduct practical security risk assessments and prioritize risks based on impact, likelihood, and control effectiveness.
- Design proportionate security controls for facilities, operations, events, sensitive areas, and critical assets.
- Strengthen access control, incident response, escalation procedures, security communication, and crisis coordination.
- Integrate security risk management with business continuity, emergency response, compliance, governance, and operational resilience.
- Use security performance indicators, incident data, audits, and lessons learned to improve security programs.
- Develop a practical security risk management roadmap aligned with institutional priorities and operational realities.

## Instructor Profile

The course will be delivered by an internationally certified expert with extensive practical and consulting experience. The instructor brings deep professional knowledge in security risk management, threat assessment, vulnerability analysis, physical security, protective planning, incident response, crisis coordination, business continuity, governance, and organizational resilience. The training approach combines executive-level insight with practical tools and real-world application, ensuring participants gain methods they can immediately implement within government entities, ministries, public sector organizations, large corporations, critical infrastructure environments, industrial facilities, and complex operational settings.

# Contact Us

For registration inquiries, upcoming dates, or group pricing, please contact us:

| | |
|---|---|
| **Website** | www.skillslab-training.com |
| **Email** | info@skillslab-training.com |
| **WhatsApp** | +966 559 653 447 |

**Generated by Skillslab Training**

info@skillslab-training.com | WhatsApp: +966 559 653 447

www.skillslab-training.com