Security & Law Enforcement · SL469

# Security Risk Assessment & Management

| Duration | Category | Ref |
|---|---|---|
| **1 Week** | **Security & Law Enforcement** | **SL469** |
| **Language** | **Certificate** | |
| **English** | **Certificate of attendance** | |

## Introduction

Organizations face a wide range of security threats that can affect their people, assets, facilities, operations, and business continuity. Effective security risk management enables organizations to identify potential threats, evaluate vulnerabilities, and implement appropriate measures to minimize their impact.

The Security Risk Assessment & Management course provides participants with a structured understanding of the principles and methodologies used to identify, assess, and manage security risks.

The course explores risk assessment frameworks, threat identification, vulnerability analysis, risk mitigation strategies, and the development of effective security risk management plans.

Participants will gain practical knowledge of how security risk assessment supports informed decision-making, strengthens security controls, and enhances organizational resilience.

## Course Objectives

### By the end of this course, participants will be able to:

- Understand the fundamental principles of security risk assessment and management.
- Identify potential security threats, hazards, and vulnerabilities.
- Evaluate the likelihood and potential impact of security risks.
- Understand security risk assessment methodologies and frameworks.
- Develop appropriate risk mitigation and treatment strategies.
- Prioritize security risks based on their potential consequences.
- Understand the role of security controls and preventive measures.
- Develop and maintain security risk registers and management plans.
- Monitor security risks and support continual improvement.

## Target Audience

### This course is designed for:

- Security Managers and Department Heads.
- Security Supervisors and Team Leaders.
- Security Officers and Operations Personnel.
- Corporate Security Professionals.
- Risk Management Professionals.
- Facility and Asset Protection Managers.
- Business Continuity and Crisis Management Professionals.
- HSE, Compliance, and Quality Professionals involved in security risk management.

Recommended level: Introductory to Intermediate.

No previous formal experience in security risk assessment is required.

## Course Outline

### Day 1

### Fundamentals of Security Risk Management

- Introduction to security risk assessment and management.
- Understanding security threats, vulnerabilities, and risks.
- The relationship between threats, assets, vulnerabilities, and consequences.
- Security risk management principles and frameworks.
- Understanding organizational context and security objectives.
- Roles and responsibilities in security risk management.
- Establishing a security risk management approach.

### Day 2

### Threat Identification and Vulnerability Assessment

- Identifying potential security threats and hazards.
- Internal and external security threats.
- Identifying critical assets and resources.
- Understanding vulnerabilities and weaknesses.
- Threat assessment methodologies.
- Vulnerability assessment principles.
- Gathering and analyzing security-related information.
- Developing a security threat profile.

### Day 3

### Security Risk Assessment Methodologies

- Understanding the security risk assessment process.
- Evaluating likelihood and potential impact.
- Qualitative and quantitative risk assessment approaches.
- Risk rating systems and assessment matrices.
- Risk prioritization and classification.
- Identifying existing security controls.
- Assessing the effectiveness of current security measures.
- Developing a security risk register.

### Day 4

## Risk Treatment and Mitigation Strategies

- Understanding security risk treatment options.
- Risk avoidance, reduction, transfer, and acceptance.
- Developing security risk mitigation plans.
- Preventive and corrective security controls.
- Physical, procedural, and operational security measures.
- Resource allocation and implementation priorities.
- Managing residual risks.
- Communicating security risks to management and stakeholders.

## Day 5

## Monitoring, Reporting, and Continual Improvement

- Monitoring and reviewing security risks.
- Maintaining and updating security risk registers.
- Security risk reporting and management dashboards.
- Key Risk Indicators (KRIs) and performance monitoring.
- Reviewing the effectiveness of mitigation measures.
- Managing emerging and changing security threats.
- Integrating security risk management into organizational planning.
- Developing a structured security risk management framework.
- Course review and knowledge consolidation.

### Ask us for a date for this course

https://www.hplustraining.com/categories/security-law-enforcement/SL469

training@hplustraining.com · +44 74 0108 8599 · +90 539 827 59 14