BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Certificate in Security Management

Course Introduction

This course is designed to provide participants with essential knowledge and practical skills for manag

Throughout the training program, participants will engage in interactive lectures, case studies,managin

By the end of the program, participants will be equipped with the knowledge and skills necessary to de

Target Audience

1. Security Manager
2. Information Security Analyst
3. Cybersecurity Consultant
4. IT Security Specialist
5. Risk Management Analyst
6. Security Operations Center (SOC) Analyst
7. Compliance Officer
8. Chief Information Security Officer (CISO)
9. Penetration Tester (Ethical Hacker)
10. Security Auditor
11. Incident Response Analyst
12. Network Security Engineer
13. Fraud Investigator

Learning Objectives

- Gain a comprehensive understanding of security management principles, including the roles, responsibilities, and legal frameworks governing security operations.

- Apply techniques for conducting effective risk assessments, analyzing security vulnerabilities, and developing risk mitigation strategies to protect organizational assets and personnel.
- Identify and implement appropriate access control measures, physical security protocols, and crisis management procedures to safeguard facilities and mitigate security threats.
- Recognize and apply investigation techniques, including interviewing, evidence collection, and incident management, to address security breaches and conduct thorough security investigations.
- Stay informed about the latest security technology advancements and emerging trends in security management, enabling proactive adaptation and integration of innovative security solutions into organizational practices.

Course Outline

- **Day 01**

  Introduction to Security Management

  - Overview of Security Management: Roles, Responsibilities, and Importance
  - Understanding Security Policies and Procedures
  - Legal and Regulatory Frameworks in Security Management
  - Introduction to Risk Management Principles in Security
- **Day 02**

  Risk Assessment and Mitigation

  - Conducting Risk Assessments: Identification, Analysis, and Evaluation
  - Developing Risk Mitigation Strategies and Action Plans
  - Implementing Security Controls and Countermeasures
  - Crisis Management and Emergency Response Planning
- **Day 03**

  Access Control and Physical Security

  - Access Control Principles and Techniques
  - Security Measures for Physical Protection: Perimeter Security, Alarms, and CCTV
  - Visitor Management and Employee Identification Systems

- Securing Facilities and Assets: Locks, Keys, and Safes

- **Day 04**

  Investigation Techniques and Incident Management

  - Conducting Security Investigations: Procedures and Best Practices
  - Interviewing Techniques and Interrogation Methods
  - Evidence Collection and Preservation
  - Incident Management and Reporting

- **Day 05**

  Security Technology and Emerging Trends

  - Overview of Security Technology: Biometrics, Access Control Systems, and Surveillance Technology
  - Emerging Trends in Security Management: Cybersecurity, IoT Security, and AI
  - Integrating Technology into Security Operations
  - Future Directions in Security Management and Professional Development Opportunities

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
June 16, 2025	June 20, 2025	5 days	4250.00 $	UAE - Dubai
Aug. 17, 2025	Aug. 21, 2025	5 days	2150.00 $	Virtual - Online
Sept. 8, 2025	Sept. 12, 2025	5 days	5950.00 $	USA - Los Angeles
Dec. 29, 2025	Jan. 2, 2026	5 days	4250.00 $	UAE - Dubai