BOOST
THE LEADING TRAINING PROVIDER

Administration and Office Efficiency

Introduction To Developing Security Management Plans

Course Introduction

The Certified Security Management Professional (CSMP) is a 12-module training program designed to provide “Louvre Abu Dhabi” employees with the essentials of managing security in a corporate environment. This training will help participants

develop their knowledge and management skills in the critical domains of security, and let them explore the critical areas of corporate security management and current best practices.

Target Audience

- Security Managers
- Risk Management Professionals
- Facility Managers
- Corporate Security Officers
- Safety and Security Consultants
- IT Security Professionals
- Human Resources Managers involved in security policies
- Emergency Response Coordinators
- Law Enforcement Officers transitioning to corporate security roles
- Professionals responsible for safeguarding organizational assets and personnel

Learning Objectives

- Gain an understanding of how HR policies and procedures fit into your organization and how they affect employee relations.
- Improve business performance and employee effectiveness through clear, fair and lawful HR policies and procedures which help maintain and uphold the morale of staff.

- Align the terms and conditions of employment with the remuneration strategy and develop detailed employment contracts to improve employer branding and employee engagement.
- Identify practical ways of developing an effective channel of communication with all employees through the HR Policies and Procedures Manual.
- Develop the skills and expertise needed to produce clear and coherent policy and procedure documents.
- Gain a comprehensive understanding of the different security domains that security professionals need to be aware of for successful management.
- Identify and analyze risks by evaluating threat likelihood, impact and vulnerability.
- Understand crime motivation theories and design crime prevention actions to be applied in the workplace.
- Recognize the daily nuts and bolts of managing a security program.
- Develop security management skills and lead the security team successfully.
- Explore and apply the tools, templates, models and best practices in optimizing security management and design to get the best return on investment.
- Master the essential elements of a perimeter design basis threat, design, civil works, fencing, lighting, surveillance, intrusion detection for an effective perimeter protection plan.
- Demonstrate ability to manage access to buildings and proper use of video surveillance for protection.
- Identify practice principles to optimize protection against a wide range of threats related to terrorism.
- Effectively protect organization’s information.
- Mitigate a range of risks to personnel, including workplace violence, armed robbery, active shooters, threats to overseas travelers and expatriates, kidnap, etc.

Course Outline

- **01 Day One**

Module 1: Security Risk Analysis

  - Determining and analyzing risks

- Prioritize security risk by evaluating threat likelihood, impact and vulnerability.

Module 2: Crime Prevention

- Crime motivation theories
- Crime prevention theories that you can apply to your workplace

Module 3: Managing the Security Function

- The daily nuts and bolts of managing a security program
- Model for interacting with the business
- Best practices for getting the best out of human security resources

• 02 Day Two

Module 4: Leadership and Management Core Skills

- Management skills
- How to develop management into leadership.

Module 5: Security Design, Evaluation and Surveying

- Tools, templates, models and good practice in how to optimize security management and design to get the best return on investment.

Module 6: Perimeter Protection

- The essential elements of a perimeter (design basis threat, design, civil works, fencing, lighting, surveillance, intrusion detection, etc.)

• 03 Day Three

Module 7: Protecting Buildings

- Buildings security, addressing design, security vulnerability analysis, core security principles, structural hardening, locking systems and critical control, intrusion detection, surveillance, etc.
- The different security characteristics of old and new buildings, and multi-tenant buildings.

Module 8: Access Management

- Access management and automated access control systems.
- Open hardware, card technology, biometrics, and vehicle control considerations.
- Contraband detection.

• 04 Day Four

Module 9: Video Surveillance (CCTV)

- Image acquisition, from the transmission to storage.
- Negotiate with suppliers and installers to get the best value for money and maximum risk reduction.

Module 10: Facility Counterterrorism

- Protecting facilities in many different environments.
- Set of ethical practice principles to optimize protection against a wide range of threats.
- Addressing dangerous threats.
- Mitigating the danger from marauding terrorist firearms attacks.

• **05 Day Five**

Module 11: Protection of Information

- Protect information in its many forms, from know-how, through hardcopy to digital data.
- The extent of the threat to business from communications intercept.

Module 12: Protection of At-Risk Personnel

- Identifying those at elevated risk.
- How to effectively mitigate a range of risks to personnel, including workplace violence, armed robbery, active shooters, threats to overseas travelers and expatriates, kidnap, etc.

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
May 12, 2025	May 16, 2025	5 days	4250.00 $	UAE - Dubai
July 21, 2025	July 25, 2025	5 days	4950.00 $	Malaysia - kuala lumpur
Dec. 22, 2025	Dec. 26, 2025	5 days	4250.00 $	UAE - Dubai