Industrial Security Management

28 March – 1 April 2027
Cairo (Egypt)



Industrial Security Management

Ref: 328780_227710 **Date:** 28 March – 1 April 2027 **Location:** Cairo (Egypt) **Fees:** 4900 GBP

Why This Course

Industrial facilities face an evolving spectrum of security challenges — from physical intrusions and insider threats to cyber risks targeting operational systems.

Maintaining security in these complex environments requires strategic planning, technical expertise, and leadership capability to protect critical operations, assets, and personnel.

The Industrial Security Management program provides a structured, multi-dimensional approach to managing security in industrial settings.

It combines risk assessment, security design, crisis response, and compliance frameworks to ensure operational resilience and continuity.

Through real-world case studies, interactive workshops, and security simulations, participants will learn to build and manage comprehensive security systems that align with organizational goals, safety standards, and global best practices.

What You'll Learn and Practice

By joining this program, you will:

- Understand the principles and framework of industrial security management.
- Learn to assess, design, and implement integrated physical and technical security systems.
- Develop skills in security risk assessment and vulnerability management.
- Explore access control, surveillance, and perimeter protection technologies.
- Gain knowledge of emergency planning, crisis response, and business continuity.
- Learn to manage insider threats, supply chain risks, and regulatory compliance.
- Build leadership capability in fostering a security-aware organizational culture.
- Apply lessons from global case studies and industrial security incidents.



The Program Flow

Day 1: Fundamentals of Industrial Security

- Understanding industrial security in the context of operational continuity.
- Types of threats: physical, technological, human, and environmental.
- Principles of deterrence, detection, delay, and response.
- Security roles, responsibilities, and governance structures.
- Case study: Security management transformation in a petrochemical facility.

Day 2: Risk Assessment and Security Planning

- Risk identification, threat modeling, and vulnerability assessment.
- Security risk matrix development and prioritization.
- Integration of risk management with safety and operational systems.
- Security master planning and policy development.
- Workshop: Conducting a security risk assessment for a manufacturing site.

Day 3: Physical and Technical Security Systems

- Facility protection: access control, barriers, and intrusion detection systems.
- Surveillance and monitoring technologies CCTV, analytics, and sensors.
- Security integration with fire, safety, and control systems.
- Perimeter and critical infrastructure protection design.
- Practical session: Designing a layered physical security system.

Day 4: Human Factors, Emergency Response, and Compliance

- Managing human-related risks — insider threats and social engineering.
- Training and awareness for a proactive security culture.
- Emergency management, crisis communication, and evacuation planning.
- Security auditing, documentation, and compliance with international standards ISO 28000, ISPS, NIST.
- Simulation: Managing a coordinated emergency and security breach scenario.

Day 5: Strategic Leadership and Future Security Trends

- Building leadership competency in industrial security management.
- Cross-functional collaboration with safety, IT, and facility teams.
- Cyber-physical security convergence and the rise of smart surveillance.
- ESG, ethics, and governance in industrial security operations.
- Group project: Developing a comprehensive industrial security management plan.



Individual Impact

- Build a strategic and technical understanding of industrial security systems.
- Strengthen analytical and problem-solving skills for risk mitigation.
- Gain confidence in leading cross-functional security and response teams.
- Learn to integrate technology, policy, and human factors in security design.
- Enhance professional credibility as a trusted security and risk management expert.

Work Impact

- Improve asset protection, operational reliability, and regulatory compliance.
- Reduce exposure to physical and operational security risks.
- Foster a culture of vigilance, accountability, and preparedness.
- Strengthen coordination between the safety, facility, and IT departments.
- Enhance business continuity and crisis resilience across operations.

Training Methodology

This program blends conceptual understanding, applied analysis, and scenario-based learning to ensure practical readiness and strategic capability.

Learning methods include:

- Interactive sessions led by security and risk management experts.
- Case studies from industrial, energy, and manufacturing sectors.
- Risk assessment workshops and simulation exercises.
- Group discussions on crisis leadership and human factors.
- Framework templates and audit toolkits for practical implementation.

Beyond the Course

Upon completion, participants will be equipped to design, lead, and sustain integrated security management programs that protect people, assets, and operations.

Graduates of this program will emerge as industrial security leaders — capable of anticipating threats, ensuring resilience, and building secure, compliant, and sustainable operational environments.

