Course - API 780 – Security Risk Assessment Methodology

Duration - 5 Days

About the Course

This course provides comprehensive knowledge and practical guidance on conducting **Security Risk Assessments (SRA)**using the methodology defined in American Petroleum Institute (**API) 780**. Participants will learn how to systematically identify security threats, analyze vulnerabilities, evaluate risks, and recommend effective countermeasures for protecting critical infrastructure and industrial facilities.

The training explains how to apply a **structured, team-based methodology** to evaluate risks to personnel, facilities, information, and operations within the petroleum, petrochemical, and other critical infrastructure sectors.

Through case studies, exercises, and practical examples, participants will develop the skills necessary to perform professional SRAs and support organizational security management decisions.

Learning Outcomes

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

1. Understand the principles and structure of **API 780 Security Risk Assessment methodology**.
2. Identify critical assets and characterize facility operations.
3. Conduct structured **threat identification and analysis**.
4. Evaluate **vulnerabilities in physical and operational security systems**.
5. Perform **risk analysis using likelihood and consequence evaluation**.
6. Develop **risk mitigation strategies and security countermeasures**.
7. Prepare professional **Security Risk Assessment reports**.
8. Integrate SRA outputs into **security management and facility protection plans**.

Target Audience

This course is designed for professionals involved in **security, risk management, and critical infrastructure protection**, including:

- Security Managers and Security Officers
- Risk Management Professionals
- Oil & Gas Facility Managers
- Physical Security Consultants
- Safety and HSE Managers
- Critical Infrastructure Protection Specialists
- Engineers and Operations Managers
- Law Enforcement and Government Security Professionals
- Corporate Security and Asset Protection Professionals

5-Day Detailed Course Outline

Day 1 – Introduction to API 780 and Security Risk Assessment

Module 1: Overview of Industrial Security Risk

- Security challenges in petroleum and petrochemical industries
- Importance of Security Risk Assessment (SRA)
- Security vs Safety risk management
- Security threats to critical infrastructure

Module 2: Introduction to API 780 Standard

- Scope and objectives of API 780
- Security terminology and definitions
- Key principles of security risk management
- Role of SRA in corporate security programs

Module 3: SRA Methodology Framework

- Overview of the API 780 methodology
- The five-step risk assessment process

- Roles and responsibilities of the SRA team
- Planning and preparation for SRA

Day 2 – Facility Characterization and Asset Identification

Module 4: Step 1 – Facility Characterization

- Understanding facility operations
- Asset identification and categorization
- Critical asset determination

Module 5: Asset Criticality and Impact Analysis

- Asset value and attractiveness
- Operational dependencies and interdependencies
- Identifying critical infrastructure elements

Module 6: Asset Documentation

- Facility layout analysis
- Process flow and operational analysis
- Identifying sensitive information and data systems

Practical Exercise

- Asset identification and facility characterization

Day 3 – Threat Assessment

Module 7: Step 2 – Threat Identification

- Threat landscape for industrial facilities
- Types of threats:
    - Terrorism
    - Sabotage

- Insider threats
- Theft and diversion
- Cyber-physical attacks

Module 8: Threat Characterization

- Threat sources and adversaries
- Target attractiveness analysis
- Threat likelihood determination

Module 9: Scenario Development

- Developing credible attack scenarios
- Threat scenario modeling
- Scenario documentation

Practical Exercise

- Threat scenario development workshop

Day 4 – Vulnerability Assessment and Risk Evaluation

Module 10: Step 3 – Vulnerability Assessment

- Identifying weaknesses in security systems
- Physical security vulnerabilities
- Operational and procedural vulnerabilities
- Human factor vulnerabilities

Module 11: Security System Analysis

- Layers of protection concept
- Access control and surveillance systems
- Security procedures and emergency response capability

Module 12: Step 4 – Risk Evaluation

- Risk equation in API 780
- Consequence analysis
- Likelihood determination
- Risk ranking and prioritization

Day 5 – Risk Treatment and SRA Implementation

Module 13: Step 5 – Risk Treatment

- Security countermeasures and mitigation strategies
- Evaluating security upgrades
- Cost-benefit analysis of countermeasures

Module 14: Security Risk Management

- Integration with security management systems
- Security performance monitoring
- Continuous improvement of security programs

Module 15: Documentation and Reporting

- Preparing an SRA report
- Communicating results to management
- Action planning and follow-up