CONCEPT

Security Risk Assessment (SRA) Methodology: API 780 Approach and Access Control

Security Risk Assessment (SRA) Methodology: API 780 Approach and Access Control

Introduction:

A security risk assessment SRA that is copied from another site, scored by one person or never revisited after a plant change gives management false comfort and misdirects security spending. Security risk assessment done properly follows a repeatable method: characterise assets, rate threats, test existing countermeasures, estimate consequences, rank risk and justify each new measure. This Core Concept course takes facility security, HSE and risk managers through the five-step SRA approach described in API Standard 780, adds access control design, and ends with each participant drafting a Facility SRA Report with a Countermeasure Action Register.

Course Objectives:

- Plan an SRA study by defining its scope, boundaries, team, data sources and the five-step approach described in API Standard 780
- Characterise facility assets and rate their importance and attractiveness using consistent consequence categories
- Rate threat likelihood and assess vulnerability of existing countermeasures with structured SRA worksheets
- Rank security risk on a likelihood and consequence matrix and select countermeasures across deter, detect, delay and respond layers
- Design access control zones, authorisation rules and credential management that follow least privilege and are reviewed periodically
- Document the SRA, set its revalidation triggers and integrate security requirements into facility design and management of change

Target Audience:

- Managers responsible for the security of refineries, petrochemical plants, terminals, utilities or other industrial sites
- HSE and process safety managers who include security scenarios in site risk registers
- Enterprise and operational risk managers who must evaluate physical security risk at facility level
- Security coordinators who lead or facilitate SRA workshops and maintain SRA records
- Engineering and project managers who must include security requirements in new or modified facilities

Course Outline:

Day 1: SRA Purpose, Scope and Study Planning

- SRA Definitions: Asset, Threat, Vulnerability, Consequence and Risk
- API Standard 780 Scope and Its Five-Step Structure
- SRA Study Boundaries: Fixed Sites, Pipelines and Mobile Operations
- Multidisciplinary SRA Team Charter and Data Request List
- Existing Security Documentation Gap Check Before the Study

Day 2: Asset Characterisation, Consequence Analysis and Threat Rating

- Asset Register for Process Units, Control Buildings, Storage and Utilities
- Consequence Categories: Casualties, Environmental Release, Production Loss and Reputation
- Target Attractiveness Scoring for Characterised Assets
- Threat Source Categories and Credible Scenario Statements for Defensive Review
- Threat Likelihood Rating Scale and Evidence Sources

Day 3: Vulnerability Assessment and Risk Ranking

- Vulnerability Worksheet for Existing Security Measures
- Countermeasure Performance Review Across Deter, Detect, Delay and Respond
- Likelihood and Consequence Risk Matrix Calibration
- Risk Ranking Workshop Facilitation and Scoring Consensus
- Residual Risk Statement and Management Acceptance Criteria

Day 4: Countermeasure Selection, Access Control Design and Security in Design

- Countermeasure Options Analysis with Effectiveness and Cost Comparison
- Access Control Zoning Plan from Public Areas to Restricted Process Areas
- Authorisation Matrix, Least Privilege Rules and Credential Life Cycle
- Periodic Access Rights Review and Access Event Log Analysis
- Security Requirements in Front-End Design and Plot Plan Review

Day 5: SRA Case Study and Facility SRA Report

- Process Plant Case: Complete SRA Worksheet Set from Characterisation to Ranking
- Terminal Case: Countermeasure Package and Access Control Zoning Proposal
- SRA Report Structure, Confidentiality Handling and Distribution List
- Revalidation Triggers: Management of Change, Incidents and Threat Level Shifts
- Own-Site Facility SRA Report and Countermeasure Action Register Draft and Peer Challenge

Skills You Will Gain:

- SRA Study Planning
- Asset Characterisation
- Threat Likelihood Rating
- Vulnerability Worksheet Analysis
- Security Risk Ranking
- Countermeasure Options Analysis
- Access Authorisation Design
- SRA Revalidation Management

Why Attend This Course:

- Return with a Facility SRA Report and Countermeasure Action Register drafted for a site you are responsible for
- Replace one-person, copied risk scores with a documented team method that management and auditors can follow
- Show which proposed security measures reduce the highest ranked risks and which add cost without benefit
- Test your scoring scales and access control rules against peers from oil and gas, chemicals, utilities and logistics

Conclusion:

A security risk assessment is only useful when its method is transparent and its results drive decisions. The course moves from SRA scope and team planning, through asset characterisation, consequence analysis and threat rating, to vulnerability worksheets, risk ranking and residual risk acceptance. It then turns to countermeasure selection, access control zoning and authorisation, and security requirements in design. The final day applies the method to process plant and terminal cases and produces a Facility SRA Report with a Countermeasure Action Register and clear revalidation triggers.