
Oil and Gas Security Risk Assessment Training Course: Threats, Vulnerabilities and Protection Plans

21 – 25 June 2027
Amsterdam





Oil and Gas Security Risk Assessment Training Course: Threats, Vulnerabilities and Protection Plans

Ref: 588_30471 **Date:** 21 – 25 June 2027 **Location:** Amsterdam **Fees:** 4800 GBP

Programme Summary

Oil and gas security risk assessment is the subject of this one-week training course for security, operations and asset managers in energy companies, ending in a facility security risk and protection plan for one site. Facilities, pipelines and terminals face deliberate threats, and weak links between asset value, threat and protection lead to spending in the wrong places. The programme moves from asset ranking through vulnerability review to risk ranking and response, applying each step to a site of the participant's own. Mars Training Centre UK delivers this programme on oil and gas security risk assessment to mixed-organisation cohorts.

The Business Case

Where assets are not ranked by consequence and threats are not tied to real access routes, controls are placed unevenly and gaps stay open. Managers who can characterise assets, test vulnerabilities, rank risks and plan layered protection direct limited budgets to the exposures that matter.

- Security Risk Exposure: Falls as credible threats are matched to the assets they can reach.
- Protection Spending Efficiency: Improves as countermeasures are chosen against ranked risks.
- Incident Response Readiness: Improves as escalation steps are agreed and rehearsed in advance.

Principles and Evidence Base

- API Standard 780: The security risk assessment method for the petroleum and petrochemical industry underpins the asset, threat and vulnerability work in Sessions 1 to 3.
- ISO 31000: The risk management process of context, assessment, treatment and monitoring structures the programme from Session 1.
- Risk register: Scoring likelihood against impact guides the ranking in Session 3.
- Layered protection: Deterring, detecting, delaying and responding frames the planning in Session 4.

Intended Participants

- Security managers who answer for the protection of energy facilities.
- Operations and site managers who carry the consequence of a security incident.
- Asset and pipeline managers who oversee remote or distributed infrastructure.
- Risk and business continuity leaders who set the risk tolerance for sites.
- Project and contractor managers who control access and third-party exposure.

Typical functions include corporate security, facility operations and enterprise risk in energy and petrochemical companies.



Learning Outcomes

1. Participants will be able to construct an asset register ranked by consequence of loss.
2. Participants will be able to diagnose credible threat scenarios against a facility.
3. Participants will be able to evaluate site vulnerabilities along access routes and perimeters.
4. Participants will be able to prioritise security risks using a likelihood and impact register.
5. Participants will be able to compare countermeasure options within a layered protection model.
6. Participants will be able to justify a facility protection plan to a senior committee.

Programme Structure

Day 1: Oil and Gas Security Risk Assessment Foundations

What is being protected, and from whom?

- Asset Characterisation Register
- Consequence Ranking Scale
- Threat Actor Profile Sheet
- ISO 31000 Risk Process Map
- Security Risk Question Brief

Day 2: Threat and Vulnerability Analysis

Where can a credible threat reach a critical asset?

- Threat Scenario Library
- Site Vulnerability Walkthrough Checklist
- Access Route and Perimeter Map
- Insider and Contractor Exposure Review
- Vulnerability Findings Log

Day 3: Risk Ranking and Countermeasure Choice

Which risks need action first, and which countermeasures fit?

- API Standard 780 Risk Ranking Matrix
- Risk Register with Likelihood and Impact
- Layered Protection Model
- Countermeasure Option Table
- Residual Risk Statement

Day 4: Protection Planning and Crisis Response

How does a site detect, delay and respond to an attack?



- Deter, Detect, Delay and Respond Plan
- Pipeline and Terminal Protection Sheet
- Security and Safety Interface Chart
- Incident Escalation Protocol
- Crisis Response Exercise Script

Day 5: Applying the Tools to One Facility

Do the assessment, ranking and protection tools support one site plan?

- Applying the Session 1 Asset Characterisation Register
- Using the Session 2 Vulnerability Findings Log
- Testing the Session 3 Risk Register
- Checking the Session 4 Incident Escalation Protocol
- Completing the Facility Security Risk and Protection Plan

Methodology

The programme uses a structured exercise method built on anonymised site layouts, incident summaries, asset lists and threat briefs drawn from upstream, pipeline and terminal settings. Participants work in mixed security and operations groups on one shared facility, challenge each other's rankings and receive written facilitator feedback on each exercise set.

- Suggested activity: Ranking ten assets of a terminal by consequence of loss.
- Suggested activity: Walking a site plan to find the weakest access route.
- Suggested activity: Choosing three countermeasures against a ranked risk register.

Capstone Output

Each participant completes a facility security risk and protection plan for one site. It holds a ranked asset register, a threat and vulnerability summary, a scored risk register, a layered countermeasure set and an incident escalation protocol. The plan is used at work to brief a senior committee, set security priorities with operations and frame the next review of site protection.

Frequently Asked Questions

Is oil and gas security risk assessment suitable for managers who are not security specialists?

Yes. Oil and gas security risk assessment is taught for managers with site, asset or risk responsibility, using sample facilities in place of specialist security engineering.



Which models does oil and gas security risk assessment rest on in this programme?

Oil and gas security risk assessment rests on API Standard 780, the ISO 31000 risk process, the risk register and the layered protection model.

How is the plan from oil and gas security risk assessment used at work?

You use the facility security risk and protection plan to brief a senior committee, set security priorities with operations and frame the next review of site protection.

How does oil and gas security risk assessment differ from cyber security training?

Oil and gas security risk assessment centres on physical threats, access and response at energy sites, while cyber security training centres on protecting information systems and networks.