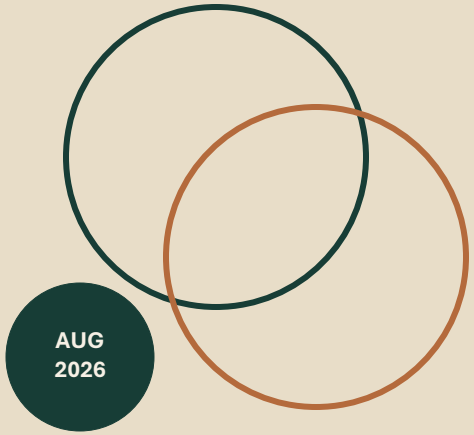
API 780 + ISO 31000

An integrated governance model for security risk decisions



CLIENT EXECUTIVE BRIEFING

Petroleum & petrochemical operations

Current references: API STD 780, 2nd ed. (2026) · ISO 31000:2018

EXECUTIVE TAKEAWAY

One governance system. One specialist assessment.

ISO 31000

sets how risk is governed, integrated and improved across the enterprise.

API 780

provides the petroleum-sector method for facility security risk assessment.

Together

create a traceable path from scenario evidence to funded countermeasures.

01

Common criteria

One risk language links security to objectives and appetite.

02

Defensible decisions

Threats, vulnerabilities and consequences support investment choices.

03

Repeatable refresh

Monitoring and review keep the assessment current as context changes.

Recommended position

Treat API 780 as the specialist security assessment embedded within the ISO 31000 framework—not as a parallel risk system.

Sources: API STD 780 (2026); ISO 31000:2018

STANDARDS AT A GLANCE

The standards solve different layers of the same decision.

ISO 31000:2018

ENTERPRISE RISK GOVERNANCE

Purpose	Create and protect value through integrated risk management.
Scope	Any organization, objective, decision or risk type.
Core structure	Principles · framework · process.
Primary users	Governing bodies, executives, managers and risk owners.
Typical outputs	Criteria, accountabilities, risk information, treatment and review.

API STD 780 · 2nd ed. 2026

SECTOR-SPECIFIC SECURITY SRA

Purpose	Support security risk assessment and countermeasure decisions.
Scope	Petroleum and petrochemical facilities; fixed and mobile applications.
Core focus	Threats · vulnerabilities · consequences · safeguards.
Primary users	Security, operations, engineering, cyber, emergency response and management.
Typical outputs	Prioritized scenarios, risk results and countermeasure recommendations.

Different altitude

Same management decision: what risk is acceptable, what must change, who funds it, and when it is reviewed.

Sources: API Webstore (2026); ISO 31000:2018 official overview

INTEGRATED ARCHITECTURE

ISO 31000 creates the operating system; API 780 runs the security assessment.

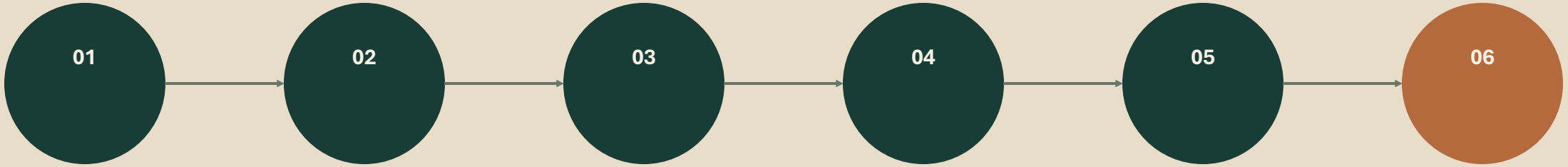
PRINCIPLES	**Value · integration · context · people · improvement**
FRAMEWORK	**Leadership · design · implementation · evaluation · improvement**
PROCESS	**Communicate · set context & criteria · assess · treat · monitor · report**

API 780 specialist security assessment

Governance outside. Sector method inside. One risk record throughout.

Sources: ISO 31000:2018 clauses 4–6; API STD 780 public description

API 780 turns security scenarios into countermeasure choices.



Scope & team

Objectives, boundaries, criteria

Assets & consequences

Critical functions and impacts

Threat scenarios

Adversary intent and pathways

Vulnerabilities

Weaknesses and existing safeguards

Risk evaluation

Compare results with criteria

Countermeasures

Select, assign and fund actions

Management outputs

- **Prioritized security scenarios**
- **Countermeasure options**
- **Residual-risk decision**
- **Owner + review trigger**

Use the licensed 2026 edition to define the detailed method, scales, documentation and quality controls for the client context.

Source: API STD 780 public summaries. Sequence shown is a non-normative implementation interpretation.

ISO 31000 CONTRIBUTION

ISO 31000 keeps risk work connected to objectives and improvement.

Create + protect value

PRINCIPLES

Direction

- Integrated with decisions
- Customized to context
- Inclusive and human-centered
- Dynamic and continually improved

FRAMEWORK

Accountability

- Leadership and commitment
- Integration into governance
- Design and implementation
- Evaluation and improvement

PROCESS

Execution

- Communicate and consult
- Set scope, context and criteria
- Assess and treat risk
- Monitor, review, record and report

Leadership implication

Security risk becomes part of planning, investment, assurance and performance—not a standalone security exercise.

Sources: ISO 31000:2018 official page and Online Browsing Platform

RECOMMENDED OPERATING MODEL

Integrate once, then repeat as conditions change.

01	02	03	04	05
Mandate & criteria	**Prioritize portfolio**	**Run API 780 SRA**	**Decide & treat**	**Monitor & refresh**
Executive / ERM	Security + operations	Multidisciplinary team	Risk owner / investment board	Assurance + site owner
Risk policy, appetite, escalation	Facility and asset screening	Scenarios, evidence, risk results	Actions, funding, residual risk	Indicators, triggers, review record

Refresh triggers material threat change · major project or MOC · security incident / near miss · control failure or assurance finding

The same criteria and record structure should follow every assessment from site evidence to executive acceptance.

Sources: ISO 31000:2018; API STD 780 public summary; CISA risk methodology guidance

Governance succeeds when decision rights and evidence are explicit.

DECISION	ACCOUNTABLE	MINIMUM EVIDENCE	ESCALATE WHEN
Risk criteria & acceptance	Executive risk owner	Approved criteria and authority limits	Exposure exceeds appetite
SRA scope & assumptions	Site / asset owner	Boundary, team, data and scenario basis	Critical information is uncertain
Treatment selection & funding	Investment decision body	Options, effectiveness, cost and dependencies	Residual risk remains material
Review cadence & triggers	Security governance forum	Indicators, incidents, change and assurance results	Context or control performance shifts

Decision quality test

Can an independent reviewer reconstruct the scenario, evidence, judgment, approval and follow-up?

Recommended model derived from ISO 31000 and API 780 public descriptions

A 90-day launch can establish a repeatable baseline.

Align

- Confirm sponsor and objectives
- Set criteria and governance
- Select pilot facility

Assess

- Mobilize multidisciplinary team
- Run pilot API 780 SRA
- Calibrate evidence and scales

Decide

- Prioritize treatments
- Assign owners and funding
- Approve residual-risk decisions

Embed

- Integrate reporting and assurance
- Track triggers and indicators
- Refresh and improve

Day 90 outcome

A governed pilot, approved treatment portfolio, named residual-risk owners, and a refresh cadence ready to scale.

Illustrative implementation roadmap; timing should be tailored to client scale and readiness

CLIENT LEADERSHIP AGENDA

Four leadership decisions unlock the program.

01 Name the sponsor

Who owns enterprise alignment, resources and escalation?

02 Define the first scope

Which facility, assets and threat context will form the pilot?

03 Approve decision criteria

What requires treatment, escalation or formal risk acceptance?

04 Set the review rhythm

Which triggers, indicators and forums keep the assessment current?

Recommended next step: confirm the four decisions, then launch a 90-day pilot using the licensed API 780 edition within the ISO 31000 governance model.

REFERENCES

Sources, status and use note

PRIMARY

American Petroleum Institute

API STD 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. 2nd edition; published 18 May 2026; current.

apiwebstore.org/standards/780

International Organization for Standardization

ISO 31000:2018 — Risk management — Guidelines. 2nd edition; published February 2018; reviewed and confirmed in 2023.

iso.org/standard/65694.html · iso.org/obp/ui/

SUPPORTING

API first-edition product announcement

api.org/~/media/files/publications/whats%20new/780%20e1%20pa.pdf

ISO/TC 262 publication note (15 Feb 2018)

committee.iso.org/sites/tc262/.../iso-310002018-has-now-published.html

CISA — Risk Assessment Methodologies

cisa.gov/resources-tools/resources/risk-assessment-methodologies

NSAI — API STD 780:2026 status listing

shop.standards.ie/en-ie/standards/api-std-780-2026-.../

USE NOTE This briefing is an executive interpretation—not an official API–ISO concordance. Use the licensed standards, applicable regulation and site-specific professional judgment for implementation.