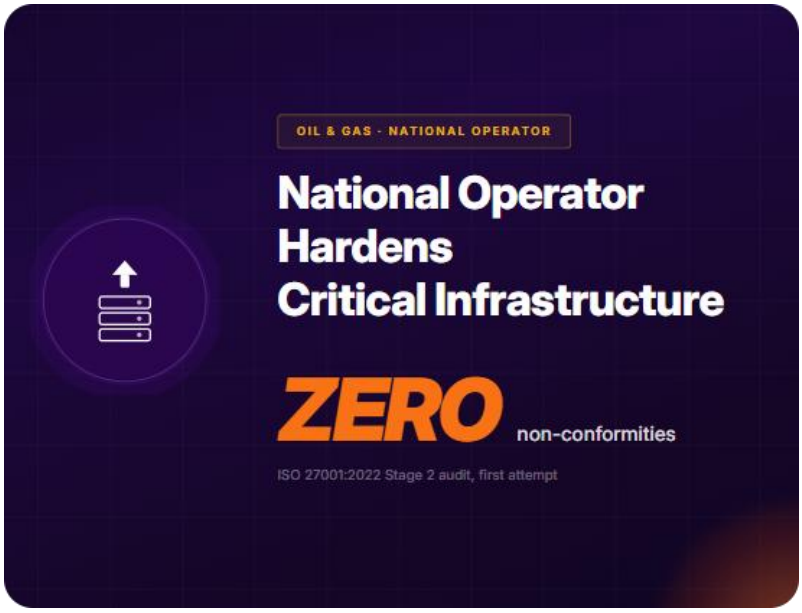
THREATSVIEW
Make it Simple

# National Oil & Gas Operator Hardens Critical Infrastructure and Earns ISO 27001:2022 Certification




## Client profile

A state-linked oil and gas operator with upstream, midstream, and downstream operations, employing roughly 8,000 staff and managing a mixed IT/OT environment that includes SCADA systems and refinery control networks.

## The Challenge

A board-mandated ISO 27001:2022 certification deadline was 12 months out, and the existing approach — spreadsheets, SharePoint folders, and ad-hoc penetration tests — could not produce the evidence trail the certification body required. Additionally, OT assets needed to be inventoried and risk-rated without disrupting plant operations.

## Why ThreatsView

ThreatsView's GRC module covered the full Annex A control set, while the Security Management Module accepted findings from passive OT scanning tools and segregated IT vs. OT asset views. The penetration testing project module allowed the security team to run an authorized red-team engagement entirely inside the platform.

## Implementation highlights

Annex A controls imported, owners assigned, and a six-month evidence collection sprint launched.

Statement of Applicability (SoA) generated from the platform.

A 10-week external penetration test tracked end-to-end in ThreatsView, with findings imported directly rather than emailed as PDFs.

## Results & impact

- Passed ISO 27001:2022 Stage 2 audit on the first attempt with zero major non-conformities.
- Cut external penetration testing reporting overhead by an estimated 60% by eliminating PDF-to-Excel re-keying.
- Built a unified risk register containing 312 risks across IT and OT, each linked to controls and treatment plans.
- Established quarterly management review packs generated automatically from platform data.

> *"We didn't just pass the audit — we built a system that keeps us audit-ready every day."*
>
> **— Chief Information Security Officer**