The top ***oil and gas challenges*** with advice for maintenance and operations leaders.

We analyze the risk factors large Oil & Gas enterprises highlight in annual reports, how risk factor disclosures relate to maintenance and operations leaders, and offer advice on how to overcome challenges.

Published	Industry	Report type
July 2026	Oil & Gas	Industry research report

CHAPTER 01

Key ***findings***.

Maintenance is typically seen as a cost center. This report makes the case that it is a form of risk control. The risks that oil and gas executives are legally required to flag to investors, volatile economics, tightening regulation and climate pressure, operational hazards, and cyber disruption, land as execution problems on real assets. The companies rarely name maintenance directly, but read the filings through a maintenance lens and it is everywhere.

We read the fiscal year 2025 risk disclosures of 13 of the largest companies in oil and gas. Six themes appear in every single filing.

Risk theme	Companies citing	Maintenance connection
Price and margin volatility	13 of 13	Cost pressure pushes leaders to get more from the assets and people they already have.
Regulation, permitting, and compliance	13 of 13	Inspections that happen on schedule, problems that get fixed, and an audit trail that proves it.
Climate and energy transition	13 of 13	Higher compliance, operating, and maintenance costs on aging assets.
Operational hazards and safety	13 of 13	Spills, leaks, fires, and mechanical failures trace back to asset integrity and execution.
Cybersecurity	13 of 13	ERP, EAM, condition-monitoring systems connect to operational technology.
Equipment failure or operational disruption	13 of 13	The core maintenance mandate: keep assets running safely.
Talent and skills	7 of 13*	Knowledge walks out the door; rework and variable execution rise.

Companies filings analyzed: ExxonMobil, Chevron, ConocoPhillips, Halliburton, Petrobras, BP, TotalEnergies, Equinor, Eni, SLB, Occidental, Marathon Petroleum, and Shell.

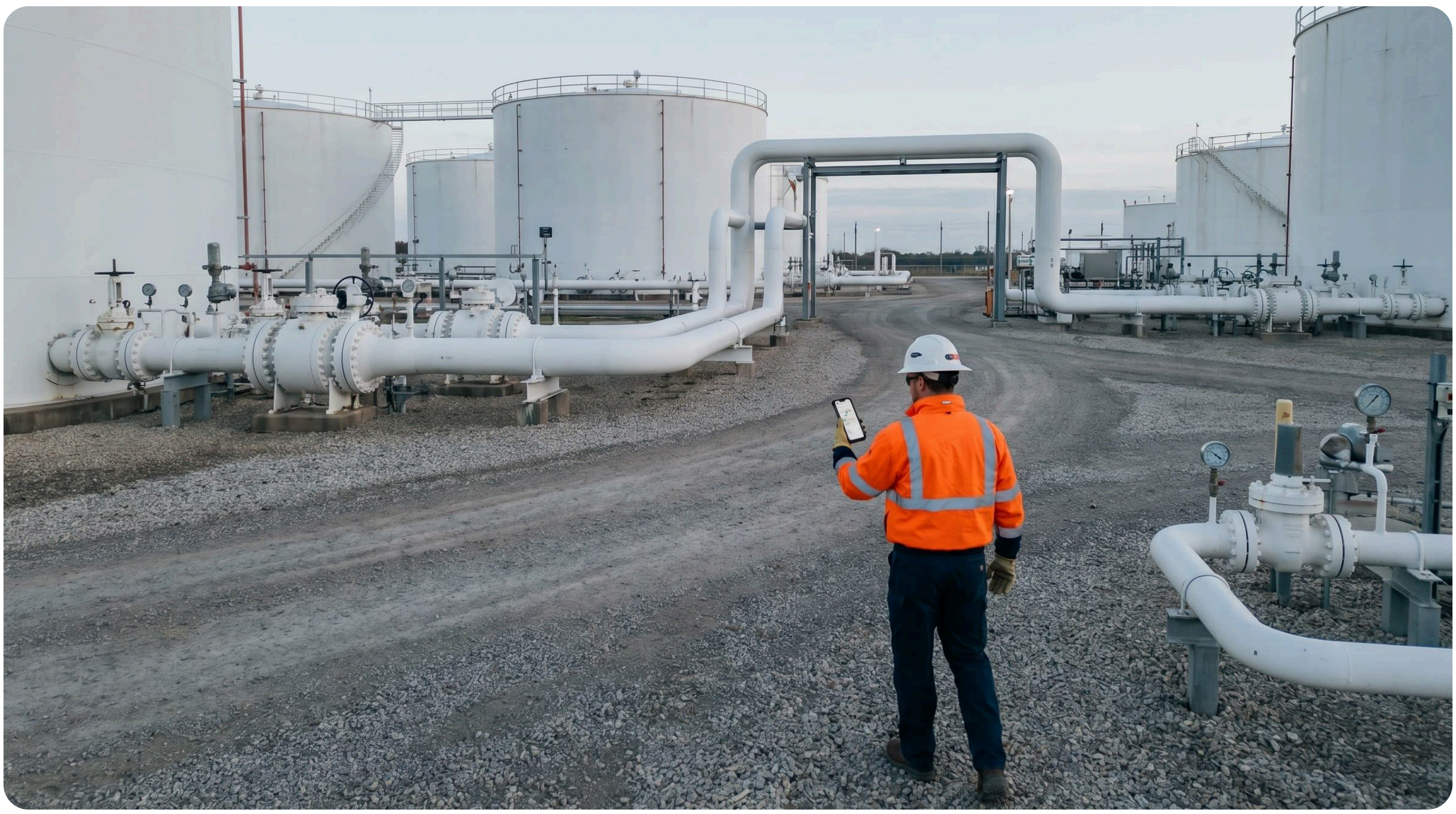
*As a distinct risk.

CHAPTER 02

Introduction: why we read the filings.

For maintenance and operations leaders to have a real voice in the room, you have to connect your objectives to the goals the business already cares about. We built this report to help you do that.

We read the fiscal year 2025 risk-factor disclosures from 13 of the largest companies in oil and gas to see what executives are consistently warning investors about. In a 10-K, that is Item 1A. In a 20-F, it is Item 3.D. These sections are what each company is legally required to disclose as material to its business.



The 13 companies analyzed: ExxonMobil, Chevron, ConocoPhillips, Halliburton, Petrobras, BP, TotalEnergies, Equinor, Eni, SLB, Occidental, Marathon Petroleum, and Shell.

The themes will not surprise you: price volatility, regulation and the energy transition, operational hazards, and cybersecurity show up again and again. What follows summarizes those themes, then translates each one into practical takeaways you can use.

CHAPTER 03

The ***risk themes*** that dominate filings.

1. Price and margin volatility

Commodity prices move fast, and so do the economics of your operations. Refiners watch crack spreads and basis differentials, upstream producers watch oil and gas prices and demand shocks, and service companies like Halliburton and SLB watch their customers' exploration and production spending.

"The level of exploration, development, and production activity is directly affected by trends in oil and natural gas prices, which historically have been volatile and are likely to continue to be volatile." — Halliburton, FY2025 Form 10-K (Item 1A)

2. Regulation, permitting, and compliance costs

Every company in the analysis flags regulatory complexity as material: environmental rules, product specifications, safety standards such as OSHA process safety management and American Petroleum Institute requirements, sanctions compliance, and shifting tax regimes. Marathon Petroleum's FY2025 filing newly references tax changes under the One Big Beautiful Bill Act.

"We have incurred and will continue to incur substantial capital, operating and maintenance, and remediation expenditures as a result of these laws and regulations." — ConocoPhillips, FY2025 Form 10-K (Item 1A)

3. Climate and energy transition

Climate-related risk appears in all 13 filings. The language varies by region and business model, but the themes are consistent: carbon regulation, shifting consumer preferences, and transition policy uncertainty. Chevron ties it directly to operational cost.

"Legislation, regulation, and other government actions related to GHG emissions and climate change could reduce demand for Chevron's hydrocarbon and other products and/or continue to increase Chevron's operational costs and reduce its return on investment." — Chevron, FY2025 Form 10-K (Item 1A)

4. Operational hazards and safety

Spills, leaks, fires, and process safety events hit reputation, license to operate, cash, and people. Every company acknowledges them. The costs land as direct (cleanup, litigation) and indirect (downtime, project delays, tighter oversight).

"Eni's future results of operations, cash flow and liquidity depend on its ability to identify and address the risks and hazards inherent to operating in those industries." — Eni, FY2025 Form 20-F (Item 3.D)

5. Cybersecurity and IT disruption

Cybersecurity appears as a material risk in all 13 filings, with most companies naming threats to both information technology and operational technology. The threats are data theft and operational disruption. Refineries run on distributed control systems, production platforms depend on SCADA, and maintenance crews use devices that connect to networks.

"We have experienced, and expect to experience in the future, cyber security threats such as denial-of-service, ransomware, hacktivism and attacks from nation state actors that target critical energy infrastructure." — Shell, FY2025 Form 20-F (Risk factors)

6. Equipment failure or operational disruption

All 13 filings name equipment failure or operational disruption as a material risk. It shows up as unplanned downtime and loss of asset integrity. Of the risk themes, this is the one that maps most directly onto maintenance, because keeping assets running safely is the work itself. Marathon Petroleum lays out the range in a single sentence.

"Our operations are subject to business interruptions, such as scheduled and unscheduled refinery turnarounds, unplanned maintenance, explosions, fires, refinery or pipeline releases, product quality incidents, power outages, severe weather, labor disputes, acts of terrorism, or other natural or man-made disasters." — Marathon Petroleum, FY2025 Form 10-K (Item 1A)

Because this theme sits at the center of what maintenance teams do, we come back to it in detail in the chapter "Risks through a maintenance lens" below, starting with what a single day of unplanned downtime actually costs.

Other themes

The filings also cover geopolitics and sanctions, customer spending cycles, reserve replacement, competition, and access to capital. These sit further from day-to-day maintenance, so we note them and move on.

The workforce gap

Six themes appear in all 13 filings. Talent is the one we've included that not all of the filings name. Seven of the 13 name talent, skills, or workforce capability as a distinct risk: Halliburton, SLB, BP, Equinor, Petrobras, Shell, and TotalEnergies.

The framing varies: Shell folds it into a culture risk ("Our people and culture"), and TotalEnergies ties it to its transition strategy ("Talent management and transition of the Company"). Marathon Petroleum discloses a distinct workforce risk too, but about union labor disruptions rather than skills. Four others mention people only in passing inside other risks; ConocoPhillips, for example, notes competition for geologists, geophysicists, and engineers inside its broader competition risk. One, Chevron, does not raise people as a risk at all.

For a sector whose frontline is aging and retiring, it is striking that nearly half the group still does not treat skills and knowledge as a risk worth naming, while every single filing names cybersecurity and climate. The work still gets done by people, and the knowledge that leaves with a retiring instrument technician is hard to replace. Where companies do name it, the language is consistent: skills gaps, capability needs, and knowledge retention, which show up in practice as slower work completion, higher rework, and more variable execution.

"Difficulties in attracting, developing and retaining people with the necessary skills and qualifications can negatively impact the implementation of our strategy." — Petrobras, FY2025 Form 20-F (Item 3.D)

Risks through a ***maintenance lens***.

The analyzed companies do not always explicitly call maintenance a risk. But the operational realities behind these disclosures, equipment failures, turnaround execution, workforce skills, regulatory compliance, and asset integrity, are maintenance problems. For each, here is what the risk looks like through an enterprise asset management and maintenance lens, and what actually helps.

Equipment reliability and unplanned downtime

Equipment failure is the risk that most obviously belongs to maintenance, and its cost is easy to underestimate until you put a number on it.

Take an illustrative refinery losing 250,000 barrels of throughput to one day of unplanned downtime. At a gross refining margin of $10 per barrel, that is about $2.5 million of lost gross margin in a day, before restart costs, overtime, and contractual penalties. The exact figure moves with your site and margin environment, but the point holds: downtime is expensive.

A simple calculation on the ***impact of downtime***.

250K	x	$10	=	$2.5M
barrels lost from one day of unplanned downtime.		gross margin per barrel the plant is earning.		minimum lost gross margin in a single day.

Advice for equipment reliability and unplanned downtime:

Running equipment to failure lets the asset choose the moment, and it chooses the worst one. The instinct is to overhaul more often, but the foundational reliability study, Nowlan and Heap's 1978 report for the US Department of Defense that established reliability-centered maintenance, showed that most failure modes are not age-related. Fixed-interval overhauls cannot prevent those failures, and intrusive maintenance can even introduce new ones. (Source: Nowlan and Heap, Reliability-Centered Maintenance, 1978)

What works is catching failures in the window before they become functional failures, what reliability engineers call the P-F interval: the time between when a problem first becomes detectable, through a vibration signature, a temperature rise, or a pressure change, and when the asset actually fails.

Condition-based and predictive maintenance use that window. You act on the equipment that is genuinely degrading and concentrate effort where a failure carries the most safety, environmental, and production risk, instead of over-servicing healthy assets and being blindsided by the rest.

In the real oil and gas world, most teams are stuck in a blend of reactive firefighting and scheduled preventive work. Not because people do not care, but because the data needed to change to a more predictive approach is not there.

Here is an overview of maintenance maturity and the approaches, systems, and decision styles required for each stage.

	Stage 1 **Firefighting**	Stage 2 **Planned**	Stage 3 **Preventive**	Stage 4 **Predictive**	Stage 5 **Intelligent**
Description	Reacting to failures.	Scheduled maintenance.	Preventing known failure modes.	Intervene before failure.	Continuously optimize.
Approach	Fix after failure.	Time and cycle based.	Condition-based.	Predict failures using condition monitoring and analytics.	Dynamic based on analytics, risks, constraints, and outcomes.
Systems	Paper and spreadsheets.	CMMS that facilitates processes.	CMMS plus Excel for investment and risk prioritization.	Sensors, historian, analytics, and an EAM system that optimizes asset use.	EAM and APM ecosystem, asset health models, and closed-loop planning.
Decision style	Led by experience.	Led by intervals.	Led by analysis.	Led by data and analysis.	Led by data.

A model for maintenance maturity.

Turnaround and shutdown execution

Refiners and integrated operators flag planned maintenance, the turnaround, as a material risk. These are high-stakes, high-cost events where schedule slips and cost overruns move quarterly results. Turnarounds slip because the plan loses the plot: scope creep, shifting priorities, and nobody working from the same version of the truth at the same time.

The economic argument is there: McKinsey has estimated that better management of shutdowns and turnarounds can deliver schedule and cost improvements of up to 30 percent. (Source: McKinsey, The upside of downtime)

Advice for turnaround and shutdown execution:

Here are some proven paths for improving turnaround and shutdown execution.

- Digitize the work: One current version of the job steps, permits, isolation notes, and safety checks, available where the work happens.
- Run the turnaround on daily reality, not yesterday's spreadsheet: Make critical-path progress visible and update it daily so issues surface early.
- Control scope like you control risk: Freeze scope and run a structured review for additions, so small changes do not add five days.
- Treat contractor coordination as a system: Early alignment, clear responsibilities, tight performance tracking, and connected planning and execution.

Workforce skills and knowledge retention

Many filings underplay this, but the operational reality does not go away. The concern is a shortage of specialized skills: refining operators, instrument technicians, reliability engineers, and field mechanics.

When your most experienced technician retires, you lose the labor hours and the decades of pattern recognition, troubleshooting instinct, and site-specific knowledge with them. If that knowledge is not captured, ideally in your procedures, checklists, and job plans, it is gone. Contractor gaps compound the problem. Weak contractor management means inconsistent workmanship, gaps in safety and compliance documentation, and poor data flowing back into your planning and reliability programs.

Advice for workforce skills and knowledge retention:

Capturing expert knowledge should be a priority for maintenance teams.

- Digital work instructions, step by step, in context, with the right documents at the point of work.
- Digital checklists with validation, to prevent missed steps and capture consistent as-found and as-left detail.
- Knowledge capture that is automatic. Photos, scans, defect codes, and short notes captured as part of completing the job, not saved as extra admin for the end of the day.

The connected worker is a common topic that taps into this risk theme. LNS Research frames connected-worker use cases around safe work procedures, agile work instructions, and training. (Source: LNS Research, Connected Worker: Connecting People and Systems to Transform Frontline Operations)

Regulatory compliance as an execution problem

Compliance is not only a documentation problem, it's also an execution problem. You need inspection schedules that actually happen, findings tracked to closure, and an audit trail that proves it. If your integrity management lives in spreadsheets, email, and stacks of paper, you are carrying compliance risk.

Advice for regulatory compliance as an execution problem:

The fix is to make the schedule, the findings, and the proof outputs of the work itself.

Digitize the inspection schedule so the work gets done on time, track every finding to closure rather than to a forgotten spreadsheet, and let the audit trail build as a by-product of the job instead of a scramble before the auditor arrives.

Cybersecurity for OT and maintenance systems

Your enterprise asset management software, your SAP maintenance instance, and your condition-monitoring systems are connected to each other and to operational technology (OT).

When IT and operations do not agree on how to secure those connections, you get one of two failures: shadow IT, where field crews use unapproved apps, or operational friction, where security controls dramatically impact people's ability to get work done.

Advice for cybersecurity for OT and maintenance systems:

Digital transformation solves a lot of these problems, and it brings security risk as software spreads through the office and the field. Aim for security without slowing the job.

- Role-based access on a least-privilege basis. People get what their work orders need and nothing more.
- Centralized identity and access governance.
- Secure-by-design integrations that stay controlled, monitored, and auditable, especially where operational technology and maintenance workflows meet.
- Offline work that does not become a security gap. Encrypt local data and sync securely.

Maximum lockdown is not practical. You need real controls that do not push crews into shadow IT because the approved software is unusable.

Data quality and master data management

Bad data is a quiet risk that underlies a lot of problems. Wrong equipment hierarchies in SAP, sync problems in the field, lag from paper-based data entry, functional locations that do not match reality, bill-of-materials errors, and phantom inventory where the system says you have the part and the shelf says you do not.

When technicians and operators cannot trust the data, they do the minimum or stop using the system, and expensive software turns into shelfware. Gartner has put the cost of poor data quality at a minimum of $12.9 million a year for the average organization, and the figure is likely higher in oil and gas. (Source: Gartner, Data Quality)

> “Gartner puts the cost of poor data quality at a minimum of **$12.9 million** a year.”

Peer-reviewed research in the Journal of Quality in Maintenance Engineering found that hard-to-use CMMS interfaces promote user error and leave people unwilling to use the system regularly. (Source: Tretten and Karim, Enhancing the usability of maintenance data management systems, 2014)

And do not assume technology covers for weak foundations: Deloitte notes that without trustworthy, well-governed master data, GenAI is prone to hallucination and incorrect recommendations. (Source: Deloitte, Why Master Data Management is "THE" Prerequisite for Enterprise AI Enablement)

CHAPTER 05

Conclusion

Risk-factor disclosures show the risks executives cannot ignore, and many of them land as execution problems on real assets. Across 13 oil and gas leaders, the same themes repeat: volatile economics, tightening regulation and climate pressure, operational hazards, and cyber disruption.

Maintenance is a form of risk control. Reliability programs, turnaround discipline, mechanical integrity, contractor effectiveness, cyber hygiene, and trustworthy asset data all protect uptime, cash flow, and license to operate.

If you take two next steps from this report, make them these:

- Build a risk-based maintenance approach: Prioritize work that reduces enterprise risk from safety, environmental exposure, production impact, and compliance.
- Connect your frontline, both ways: push the right SAP context out to technicians so the work goes faster, and capture clean execution data back so the record matches reality.

Would you like to put a number on your own downtime exposure? Our EAM software ROI calculator shows the cost of downtime and how much you could save at different EAM software adoption rates.

Let's talk

CONTACT

hello@arkyn.io

www.arkyn.io

HEADQUARTERS

St. Kongensgade 36-38

3rd floor

Copenhagen, Denmark

ABOUT THIS REPORT

This report analyzes the fiscal year 2025 risk-factor disclosures of 13 publicly listed oil and gas companies, drawn from their annual reports filed with the U.S. Securities and Exchange Commission between January and April 2026: the Form 10-K (Item 1A, Risk Factors) for U.S. filers and the Form 20-F (Item 3.D, Risk Factors) for foreign private issuers. Where a 20-F incorporates its risk factors by reference, we read the referenced annual report directly.