ETHIXBASE360

FEBUARY 2026

2026 Outlook

Navigating Third-Party Risk Management in the Pharmaceutical and Life Sciences Sector

2026 Outlook

Navigating Third-Party Risk Management in the Pharmaceutical and Life Sciences Sector

Introduction

Pharmaceutical and life sciences companies continue to operate under intense regulatory scrutiny while facing pressure to remain agile and competitive. Oversight has tightened further since the original publication of this report, even as companies are expected to accelerate innovation, manage costs, and secure increasingly fragile global supply chains.

Third-party relationships remain central to this tension. Vast networks of external partners support the journey from discovery to market, but they also extend risk far beyond organizational boundaries. When not properly managed, third-party risk can lead to compliance failures, operational disruption, reputational damage, and increased costs.

In 2026, these risks are no longer hypothetical. Environmental, social, and governance (ESG) obligations have moved from emerging expectations to enforceable requirements in several jurisdictions. Geopolitical volatility continues to expose supply-chain dependencies, complicating regulatory compliance and operational planning. In response, many pharmaceutical executives are repositioning third-party risk management (TPRM) from a defensive control to strategic infrastructure.

This shift is achievable, but it requires a clear understanding of sector-specific vulnerabilities, the regulatory direction of travel, and the operational capabilities needed to manage risk at scale.

"Pharmaceutical supply chains face rising cyber, theft and fraud risks, with inadequate real-time visibility identified as a critical vulnerability by a majority of executives."

December 2024 survey by Tive and BioPharma Dive[1]

From risk to resilience – with Ethixbase360

Sector-specific vulnerabilities

Globalized supply chains and geopolitical risk

More than half of the active pharmaceutical ingredient (API) manufacturing capacity supporting U.S. medicines resides in heightened risk markets, with India accounting for approximately 48% of active API filings and China a significant contributor to global API production.[2] With the U.S. possessing a relatively small domestic share, it underscores a strategic supply-chain vulnerability.

In recent years, enforcement attention has increasingly focused on indirect exposure. For instance, the United States' Uyghur Forced Labor Prevention Act (UFLPA), now firmly embedded in customs enforcement practice, continues to block imports unless companies can demonstrate that goods are free from forced labour.

There is a notable increase in enforcement activity at the border. U.S. Customs and Border Protection (CBP) continues to issue Withhold Release Orders (WROs) detaining goods suspected of being produced with forced labour, and their public dashboard shows that pharmaceutical companies are among the most frequently targeted.[3] These measures illustrate how insufficient traceability can translate directly into shipment detention and lost market access, reinforcing the need for proactive supply-chain due diligence and documentation.

Pharmaceutical companies with exposure through intermediaries or sub-tier suppliers face material disruption risk even in the absence of direct involvement.

Contract manufacturing and data integrity

The widespread use of Contract Manufacturing Organizations (CMOs) and Contract Research Organizations (CROs), which provide outsourced manufacturing, clinical research, and development services, allows pharmaceutical companies to scale rapidly and access specialist expertise. It also, however, extends governance risk across multiple jurisdictions, systems, and control environments.

When they enter relationships with CMOs and CROs, companies inherit variability in quality systems, audit trails, access controls, data-integrity practices, and ethics programmes. Recent industry surveys continue to show that most manufacturers view third-party governance weaknesses as a source of regulatory and reputational exposure.[5]

In a sector that depends on regulatory and patient confidence, failures in third-party oversight can quickly damage credibility and attract scrutiny.

From risk to resilience – with Ethixbase360

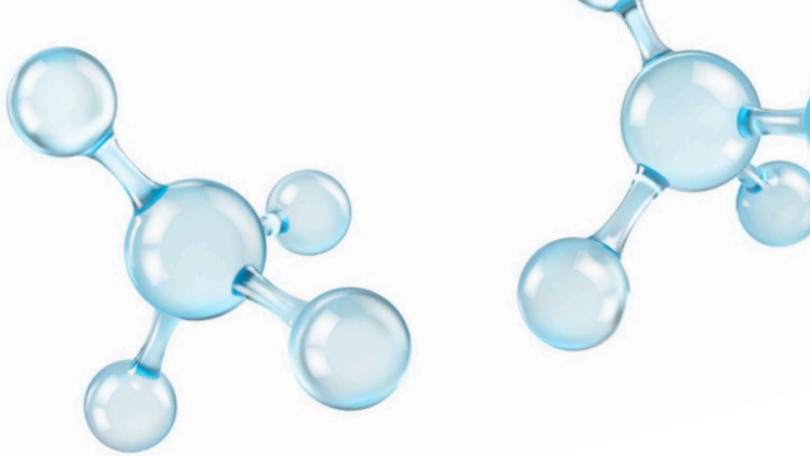
ESG and human-rights exposure

ESG risk is no longer framed as only a reputational concern. Regulatory frameworks across the European Union, the United Kingdom, Canada, and Australia now impose direct accountability on lead companies for environmental and human-rights violations across their supply chains. [6]

The European Union's Corporate Sustainability Due Diligence Directive (CSDDD), formally adopted at EU level in 2024, introduces mandatory human-rights and environmental due-diligence obligations for large companies operating in the EU. The Directive applies on a phased basis, with scope defined by employee and global turnover thresholds, and implementation dependent on national transposition. While the final text narrowed and sequenced obligations compared with earlier proposals, it still requires companies to identify, prevent, mitigate, and remediate adverse impacts across their own operations, subsidiaries, and relevant parts of their value chains.

Momentum is also building in the Asia-Pacific region. In a recently published paper[7], Australia's Anti-Slavery Commissioner recommended moving toward a mandatory, risk-based due-diligence regime and the designation of "high-risk" sectors requiring enhanced oversight, while New Zealand lawmakers are advancing modern slavery legislation with bipartisan support[8]. These developments signal that reporting-only frameworks are giving way to enforceable, risk-based expectations.

Regulators are moving towards closing historical oversight gaps, particularly where raw-material sourcing, subcontracting, or logistics providers operate in high-risk jurisdictions.



Regulatory and enforcement landscape

Regulators continue to prioritize the pharmaceutical and life sciences sector for anti-bribery, corruption, and trade-compliance enforcement. Expectations are rising, and authorities increasingly assess program effectiveness rather than policy design. The emphasis is on documented monitoring, timely remediation, clear escalation pathways, and accountable leadership.[9]

In the United States, Department of Justice (DOJ) guidance places sustained focus on demonstrable outcomes. Companies are expected to evidence continuous oversight of third parties and the ability to identify and address issues in real time. The Foreign Corrupt Practices Act (FCPA) remains the principal enforcement mechanism for overseas misconduct.[10] It is now complemented by the Foreign Extortion Prevention Act (FEPA), enacted in 2024, which criminalises the solicitation or acceptance of bribes by foreign officials, reinforcing expectations that organizations actively supervise interactions between third parties and government stakeholders.[11]

Following last year's pause in FCPA enforcement activity, the DOJ's approach has re-emerged in a more targeted form. Recent DOJ commentary and industry briefings highlight voluntary self-disclosure, cooperation credit, and closer cross-border coordination, particularly where bribery risks intersect with national security or market integrity concerns.

Across Europe, the UK Bribery Act, the recent UK Failure to Prevent Fraud (September 2025) offence, and comparable regimes maintain broad extraterritorial reach, supported by greater coordination and information sharing among enforcement bodies. With more than 40 countries now enforcing foreign bribery laws under the OECD Anti-Bribery Convention, exposure is no longer primarily a U.S. issue; parallel investigations and information sharing mean risks can surface through non-U.S. authorities even when American enforcement appears quieter.[12]

At the same time, supply-chain accountability is moving from voluntary practice to legal obligation. The EU Corporate Sustainability Due Diligence Directive (CSDDD) requires in-scope companies to identify, prevent, and remediate human-rights and environmental risks across their value chains, with supervisory oversight and potential penalties for non-compliance.[13]

China has intensified anti-corruption and competition enforcement in the healthcare and pharmaceutical sector. National campaigns through 2024–25 sustained scrutiny of commercial bribery and malpractice, while antitrust authorities have pursued price-fixing and market-division conduct. In 2025, Tianjin's antitrust authority imposed administrative penalties totalling approximately CNY 360 million on domestic pharmaceutical companies, alongside a personal fine for the scheme's organiser, and additional actions targeted improper promotional and gifting practices. Together, these cases illustrate a consistent focus on both corporate and individual accountability by the Chinese government and demonstrate that enforcement applies across domestic and foreign-invested firms alike.[14]

Human-rights trade controls are tightening in parallel. Import screening regimes modelled on the Uyghur Forced Labor Prevention Act are being implemented or expanded in multiple jurisdictions, increasing documentation and traceability requirements for raw materials and APIs.[15]

These developments point to greater expectations of transparency and control across extended supply chains. Regulators increasingly converge on three practical priorities: traceability, continuous monitoring, and demonstrable oversight.

While these requirements increase the operational burden on compliance teams, they also favour organizations that embed third-party risk management (TPRM) as core infrastructure. Programs that combine risk tiering, defensible due diligence, and real-time visibility are better positioned to maintain market access and respond to regulatory change.

"Since the first life sciences-related FCPA enforcement action in 2002, over 35 healthcare and life sciences companies have paid more than $1.5 billion in FCPA-related penalties and disgorgement."

— Charles Duross, Global Co-Chair of the FCPA & Global Anti-Corruption Practice at Morrison & Foerster LLP, and former Chief of the DOJ FCPA Unit[16]

From risk to resilience – with Ethixbase360

Third-party relationships in the pharmaceutical life cycle

The connection between the pharmaceutical life cycle's third-party touchpoints and regulatory frameworks.[17]

Lifecycle stage	Third-party relationships	Exposure
R&D & clinical trials	CROs, academic labs, data vendors. Risks: data integrity breaches, bribery, falsified results.	FCPA; FEPA; U.K. Bribery Act; Sapin II; Brazil Clean Company Act; EU CSDDD; Germany LkSG; U.K. Modern Slavery Act; Australia Modern Slavery Act; Norway Transparency Act
Regulatory approvals	Consultants, lobbyists. Risks: bribery of officials, false submissions.	FCPA; FEPA; U.K. Bribery Act; Sapin II; Brazil Clean Company Act; EU CSDDD
Manufacturing	API suppliers, CMOs. Risks: counterfeits, substandard inputs, ESG violations.	FCPA; U.K. Bribery Act; Sapin II; Brazil Clean Company Act; U.S. UFLPA; EU Forced-Labour Regulation (import bans); CSDDD/LkSG; Australia Modern Slavery Act; Competition / antitrust laws
Distribution & logistics	Wholesalers, logistics providers. Risks: diversion, falsified temperature logs, smuggling.	FCPA; U.K. Bribery Act; U.S. UFLPA; EU Forced-Labour Regulation; CSDDD/LkSG; Australia Modern Slavery Act
Sales & marketing	Agents, distributors, HCP engagement. Risks: kickbacks, sham consultancies, off-label promotion.	U.S. Anti-Kickback Statute; FCPA; FEPA; U.K. Bribery Act; CSDDD
Pharmacovigilance	Outsourced safety vendors, data processors. Risks: privacy breaches, falsified reports.	FCPA; U.K. Bribery Act; CSDDD/LkSG; U.K. & Australia Modern Slavery Acts; Modern-Slavery & Transparency Acts

From risk to resilience – with Ethixbase360

Addressing evolving regulatory priorities: practical guidance for executives

Amid these pressures, the most effective response is consistent and repeatable: focus on fundamentals that translate across jurisdictions and establish a third-party risk management (TPRM) program that is proportionate, defensible, and demonstrably effective.

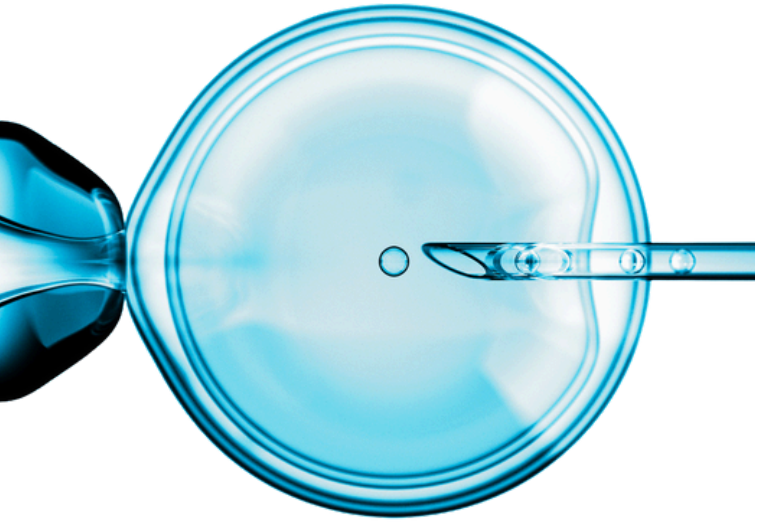
Companies should begin by ranking third parties based on geography, business activity, and government exposure, applying deeper scrutiny where risk is highest. Risk-based prioritisation concentrates resources where regulatory, operational, or reputational consequences are most material.

Technology accelerates this process, including automated screening to ESG scoring and ownership analysis, but it should support, not replace, informed human judgement.

Governance is equally critical. Assign clear executive ownership, link risk metrics to performance scorecards, and ensure board-level visibility. Regulators increasingly expect evidence of accountability as well as policy.

On ESG and human rights, strengthen supplier codes of conduct and verify compliance through audits, local partners, and documented remediation. Mapping even two tiers of suppliers typically reveals dependencies and exposures that would otherwise remain unseen. Be able to show preparation activity: develop incident playbooks, rehearse response plans, and build resilience through alternative suppliers and contingency options.

Avoid fragmentation by establishing a central risk framework that local teams can apply consistently. Replace static onboarding checks with continuous monitoring and real-time visibility. Done well, these practices not only satisfy regulatory expectations but also protect reputation, improve decision-making, and reduce long-term cost.



From risk to resilience – with Ethixbase360

Takeaways:

Prioritize credibility

In a high-trust industry, reputation depends on demonstrable compliance and consistent conduct. When operating across multiple jurisdictions, default to the strictest applicable standards.

See the whole network

Effective oversight requires visibility across third parties and sub-suppliers. Since full coverage is impractical, risk-based due diligence focuses effort where exposure is greatest and closes the most significant gaps.

Align to regulatory priorities

Heightened ESG, human-rights, and trade-compliance requirements make ethical sourcing and traceability prerequisites for market access and investor confidence.

Make culture measurable

Regulators assess behaviour as well as controls. Regular communication protocols, escalation practices, incentives, and remediation processes should reinforce ethical conduct throughout the organization and beyond to third party relationships.

Embed resilience

A sustained commitment to ethical standards and proactive oversight enables faster response to regulatory change and operational disruption.

Standardize due diligence

Shared templates, common data, and cross-functional ownership reduce duplication, improve comparability, and create defensible audit trails.

Use technology with judgement

AI and workflow automation improve speed and consistency, but human assessment remains essential for evaluating culture, reputation, and complex ownership structures. Evidence of AI controls is increasingly essential. The EU Artificial Intelligence Act (August 2024) introduces governance expectations for higher-risk AI applications, including those used in pharmacovigilance, monitoring, and third-party screening. Organizations that use AI tools in data governance, human oversight, auditability, and incident reporting will need to be able to demonstrate that automated decision-making remains explainable and compliant.

Moving beyond compliance to strategic value

For pharmaceutical companies seeking resilience, third-party risk management is no longer solely a compliance function. Digital capability supports a shift from reactive controls to entrenched infrastructure. This allows TPRM to move from being a cost centre to a foundation for operational and strategic advantage, supported by robust, repeatable, and defensible processes.

The business case for investing in a mature TPRM framework is clear:

- **Investor confidence** – ESG-aligned supply chains and demonstrable controls support access to capital and sustainable finance mandates.
- **M&A readiness** – Reliable third-party data accelerates diligence and reduces post-integration risk in a partnership-intensive sector.
- **Operational agility** – Digitised monitoring and risk visibility enable quick, urgent side steps in response to sanctions, pandemics, or geopolitical disruption, reducing disruption to a minimum.
- **Brand protection** – Proactive oversight strengthens trust with regulators, patients, and investors, protecting long-term enterprise value.

A well-designed compliance framework is a position of strength. It reduces friction, supports faster decisions, and enables resilience and sustainable growth.

Conclusion: TPRM as strategic infrastructure

In 2026, third-party risk is both a source of exposure and a source of competitive advantage. Executives who approach TPRM as a growth strategy, part of the operating system rather than a backroom compliance function, will have a competitive advantage over their peers. It requires digital-first visibility, automated onboarding, risk ranking, and continuous monitoring to identify issues early and respond more effectively.

ESG and human rights will now need to be non-negotiable and easily evidenced throughout the supply chain, while also building resilience with alternative suppliers and clear contingency plans.

Most importantly, leaders should tie TPRM to performance by including risk and resilience metrics on executive scorecards.

The updated approach should be less about adding rules and more about building trust, speed, and transparency into day-to-day decisions. If executed well, compliance spend becomes strategic capital, protecting reputation, smoothing audits, lowering the cost of change, and creating room for growth.

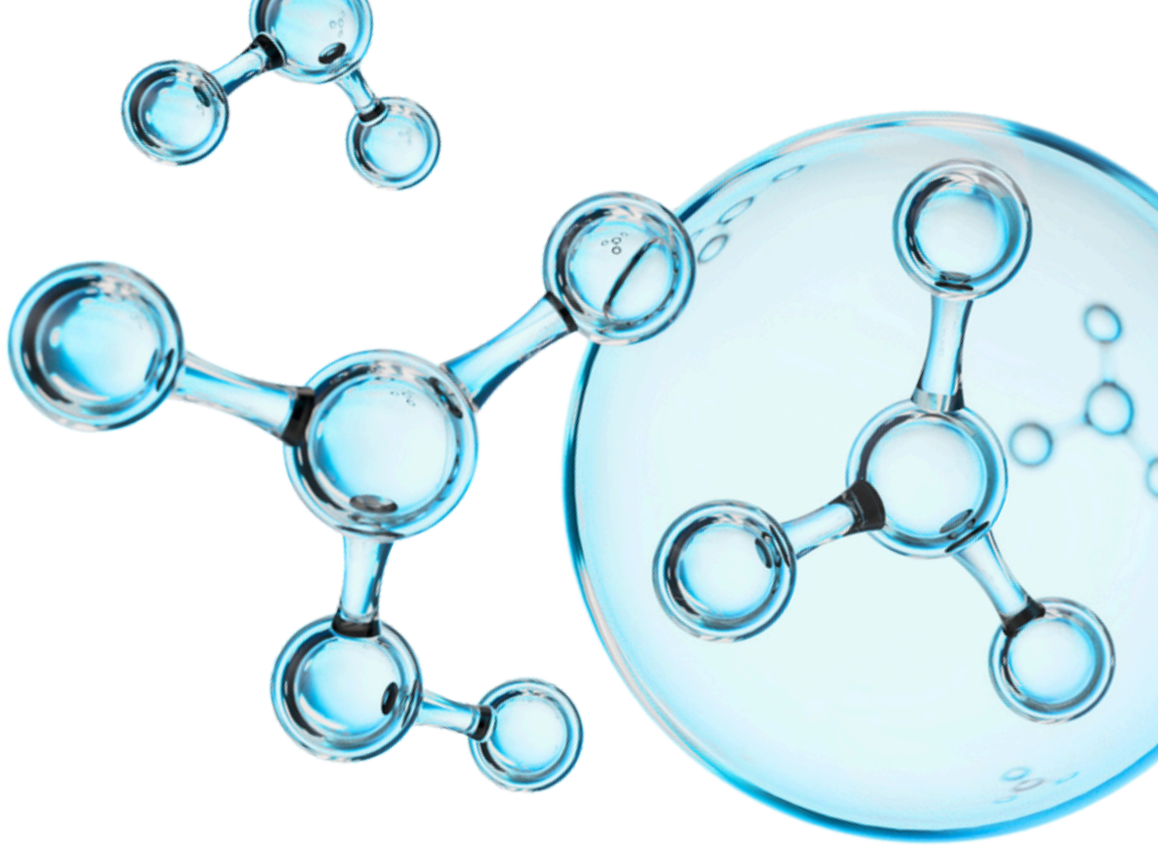
Author

James Swenson
Managing Director, Ethixbase360

James Swenson leads Ethixbase360's Enhanced Due Diligence (EDD) business from London, bringing over 20 years of experience in helping clients design, implement, and optimize third-party risk management programs. He has deep expertise in navigating complex regulatory environments and works closely with organizations to address high-risk relationships and strengthen global compliance frameworks.

James is recognized as a leading authority on anti-money laundering (AML), counter-terrorism financing (CTF), anti-bribery and corruption (ABC) risk assessments, and politically exposed persons (PEP) screening. His work focuses on delivering tailored due diligence solutions that help companies proactively manage risk, meet regulatory expectations, and build trust across their third-party networks.

From risk to resilience – with Ethixbase360



About Ethixbase 360

Ethixbase360 empowers confident third-party risk management through smart automation, expert-led due diligence, and responsive support. Our platform provides a single, connected view of global third-party risk, with insight and audit readiness built in. Designed to flex with risk and change, it adapts to shifting regulations and priorities, giving organizations control and the ability to respond at pace. Its proven configurability is backed by expert teams who bring human intelligence to every decision. Covering Anti-Bribery and Corruption, Modern Slavery, Human Rights, and Cyber, Ethixbase360 helps organizations stay resilient and agile, enabling faster decisions, greater value chain transparency, and clarity in an increasingly complex risk landscape. Learn more at **www.ethixbase360.com**.

1. Tive & BioPharma Dive, Pharmaceutical Supply Chain Visibility Survey, December 2024.
2. U.S. Food and Drug Administration, Drug Master File (DMF) and API Facility Registration Data, latest available year.
3. CBP issues WRO against Finca Monte Grande, U.S. Customs and Border Protection, January 29 2026
4. Verdantix, Third-Party Risk Management Market Insight / Industry Commentary, 2025
5. Deloitte, Global Third-Party Risk Management Survey, 2024.
6. UK Modern Slavery Act 2015; Canada Fighting Against Forced Labour and Child Labour in Supply Chains Act (Bill S-211, in force 2024); Australia Modern Slavery Act 2018
7. Commissioner's Recommendations to Strengthen Modern Slavery Laws, Anti-Slavery Commissioner, Australian Government, 30 January 2026
8. Watch: National and Labour MPs team up to get slavery bill heard after ACT objects, RNZ, 29 January 2026
9. U.S. Department of Justice, Evaluation of Corporate Compliance Programs, Criminal Division, September 2024.
10. U.S. Foreign Corrupt Practices Act, 15 U.S.C. §§ 78dd-1 et seq.
11. Foreign Extortion Prevention Act (FEPA), enacted January 2024.
12. Ethixbase360, Top Five Takeaways from the 2025 FCPA Year in Review Webinar, February 2026.
13. European Commission, Corporate Sustainability Due Diligence Directive (CSDDD) framework and implementing guidance.
14. Tianjin Municipal Administration for Market Regulation, administrative penalty announcement relating to pharmaceutical price-fixing conduct, 2025
15. U.S. Customs and Border Protection, Uyghur Forced Labor Prevention Act enforcement guidance, with comparable regimes emerging in Canada, Australia, and the European Union.
16. Morrison & Foerster, Life Sciences FCPA Enforcement Trends and Compliance Outlook, latest edition.
17. Statutes listed in the lifecycle table reflect the principal anti-corruption, human-rights, and trade-compliance frameworks applicable at each stage.

From risk to resilience – with Ethixbase360

Website LinkedIn Mail