ETHIXBASE360

MAY 2026

Third-Party Risk in an Age of Engineered Volatility and Fragmentation

CONTENTS

CHAPTER 01

The New Normal: Engineered Volatility and Fragmentation

> *"Let me be direct. We are in the midst of a rupture, not a transition....We know the old order is not coming back."*
>
> - Mark Carney, Prime Minister of Canada, excerpt from remarks at the World Economic Forum's Annual Meeting 2026 in Davos, Switzerland

When we published the first edition of this guide in 2025, we introduced readers to the Era of Perma-Crisis. One year on, the sources of that perma-crisis are becoming more clear: volatility and fragmentation, both geopolitical and economic, that are being actively engineered.

Governments are reshaping the risks facing businesses – not only directly, but also by influencing the incentives for, and behaviors of, third parties. The question is no longer who your partners are; it is how they are responding to a world where the rules are constantly changing.

In response, risk-savvy businesses that value integrity must not rely on their compliance playbooks alone. Rather, they must lean into flexibility and adaptability, guided by their values.

In this environment, third-party risk is no longer a static assessment. It is a moving target shaped by external pressure and shifting incentives.

CHAPTER 02

A Shifting Regulatory Landscape

The regulatory picture in 2026 is no more clear than the geopolitical. When regional compliance expectations move in opposite directions, the importance of ethical business leadership rises.

At the same time, while approaches differ across jurisdictions, the broader shift is clear: regulators are moving beyond disclosure toward enforcement, increasingly using trade, procurement, and market access as tools to drive compliance.

- U.S. Foreign Corrupt Practices Act enforcement remains restrained, but that is no reason to reduce compliance. The law remains in place and has a five-year statute of limitations, with proposals to extend it to 10 years. Enforcement priorities can shift quickly with changes in administration.
- The EU Corporate Sustainability Due Diligence Directive is advancing, but the Sustainability Omnibus has introduced changes to scope, timelines, and reporting requirements—creating both uncertainty and a longer runway for implementation.
- The EU Forced Labor Regulation introduces import bans and product-level enforcement, expanding regulatory reach beyond reporting into direct market intervention.
- The Uyghur Forced Labor Prevention Act in the U.S. continues to intensify, with enforcement expanding across sectors and increasing expectations for supply chain traceability.
- The UK and Australia are advancing Modern Slavery Act reforms, signaling a shift from disclosure-based regimes toward stronger due diligence obligations and penalties.
- The UK National Health Service Procurement, Slavery and Human Trafficking Regulations 2025 embed social value and environmental sustainability into supplier selection, reinforcing the role of procurement as an enforcement mechanism.

In this environment, organizations must navigate not only increasing regulatory expectations, but also divergence across jurisdictions, requiring more agile, risk-based compliance programs that can adapt as quickly as the rules themselves.

CHAPTER 03

Beneficial Ownership Considerations

Beneficial ownership is no longer a peripheral compliance issue. It sits at the center of sanctions enforcement, export controls, and third-party risk. The focus has shifted from collecting ownership data to proving, defending, and continuously monitoring who ultimately controls or benefits from a relationship.

In a fragmented and high-pressure environment, ownership structures are increasingly used to obscure exposure, through layered entities, intermediaries, indirect control, and increasingly complex cross-border networks. At the same time, organizations are operating in an environment where access to reliable ownership information can vary significantly by jurisdiction, and in some cases is becoming more restricted. Emerging regulations, including new supply chain and data-related requirements in China, are also creating additional complexity around how information can be collected, transferred, and verified across borders.

Frameworks such as the OFAC 50% rule and expanding export control expectations mean ownership is not just contextual—it is often determinative. In practice, UBO analysis can decide whether a transaction proceeds, requires escalation, or must be declined.

This reflects a broader shift from static, form-based compliance toward continuous, risk-based ownership intelligence, where organizations must navigate both heightened transparency expectations and increasingly fragmented regulatory environments.

The New Baseline

UBO due diligence can no longer be treated as a one-time onboarding step. As regulatory expectations and enforcement patterns evolve, effective programs are:

- Continuous rather than periodic
- Risk-based rather than rules-based
- Evidence-led and audit-ready
- Integrated across sanctions, trade, and third-party risk workflows
- Designed to navigate cross-border data access, transparency gaps, and conflicting regulatory requirements

CHAPTER 04

Changing Scenario for Third-Party Risk

As we have explored at Ethixbase360, third-party behavior shifts first under pressure.

In a world of engineered volatility, economic and geopolitical forces are not just increasing risk, they are reshaping incentives. Third parties are often the first to respond, adapting their behavior in ways that may reduce cost or preserve access to markets, but increase compliance and integrity risk for their partners.

For risk managers, this creates a fundamental challenge: these shifts are often subtle, difficult to detect in real time, and costly to ignore.

Periods of economic pressure, in particular, can create perverse incentives. As firms reassess margins, supply chains, and market access, compliance may be deprioritized, intentionally or otherwise.

Common patterns include:

Tariff and trade pressure
leading to manipulation of pricing structures, routing, or origin declarations

Sanctions tightening
driving the use of intermediaries or counterparties not yet on watchlists to maintain business continuity

Supply chain fragmentation
pushing companies into relationships with less-vetted or unfamiliar partners

Political and regulatory pressure on ESG
resulting in superficial compliance rather than meaningful risk management

These behaviors rarely present as overt misconduct. Instead, they emerge gradually, through changes in counterparties, transaction flows, or commercial structures, making them harder to identify through traditional due diligence alone.

If third parties are adapting faster than your controls, your compliance function risks being left in a reactive position.

At the same time, reducing compliance investment during periods of economic stress can create precisely the conditions in which these risks proliferate, limiting visibility, weakening oversight, and allowing small issues to scale into material exposure.

In this environment, effective third-party risk management is not just about identifying known risks, but about anticipating how incentives and behaviors shift under pressure.

CHAPTER 05

Geopolitical Risks in an Engineered Environment

When the sources of risk are interconnected, businesses need to deploy a wide lens, both to understand those risks and plan their responses. Major themes in 2026 include:

Conflict

- The ongoing war in Ukraine has exposed sophisticated networks for evading sanctions on Russia, such as shadow fleets, ownership layering, and intermediary switching.
- The durability of those sanctions itself is under pressure due to internal U.S., European, and Transatlantic political dynamics.
- The removal of Nicolás Maduro and the installation of an acting government in Venezuela opens up new commercial opportunities, but sanctions remain in place.
- The Iran war has disrupted shipping routes, exposed supply chain fragility, and reminded us of the importance of oil, not just in the energy mix, but throughout the economy.

Trade Fragmentation

- Governments are deploying a range of trade policies as instruments of international competition and domestic industrial development.
- US-China decoupling has accelerated, spanning sectors such as semiconductors, AI, and critical minerals.
- Trade maps and supply chains that businesses spent decades building need to be rethought, as sanctions and export controls are navigated.
- In response, friend-shoring and near-shoring are on the rise, shifting supply chains.

CHAPTER 06

Increasing Third-Party Cyber Risk and AI Considerations

Third-party cyber risk has become one of the most significant and least understood threats facing modern organizations. As businesses rely more heavily on cloud platforms, SaaS providers, and outsourced services, attackers are increasingly targeting suppliers as the most efficient route into enterprise environments.

In many cases, a single compromised vendor can provide access to multiple organizations, creating a multiplier effect where one breach leads to widespread operational, regulatory, and reputational impact.

AI is accelerating both risk detection and risk creation. Companies must pay careful attention to a range of emerging challenges, including:

- The rise of third-party cyber breaches as primary entry points into organizations
- Vendor access risk, particularly where third parties have persistent or privileged system access
- Limited visibility into vendor security environments and delayed breach detection
- AI-driven risks, including:
  - Synthetic identities
  - Rapid generation of adverse media and disinformation
  - Automation of fraud, phishing, and evasion techniques

At the same time, many organizations continue to treat cyber risk as a technical issue or a one-time onboarding check. In practice, this approach leaves significant gaps. Vendors evolve over time, introducing new systems, subcontractors, and vulnerabilities, while threat actors continuously adapt their methods.

CHAPTER 06

From Vendor Risk to Enterprise Risk

Third-party cyber risk is no longer confined to IT. It sits across compliance, procurement, legal, and risk functions, yet is often managed in a fragmented way. This lack of shared visibility can delay detection and response, allowing incidents to escalate.

Effective programs are moving toward:

- **Shared accountability across the enterprise**, with clear governance and ownership
- **Risk-based segmentation of vendors**, aligned to access, criticality, and business impact
- **Continuous monitoring**, rather than point-in-time assessments
- **Contractual enforceability**, including defined security obligations and response requirements

In this environment, managing third-party cyber risk is not about preventing every breach. It is about building the visibility, control, and resilience needed to detect issues early, respond effectively, and limit the impact when incidents occur.

CHAPTER 07

Emerging ESG and Human Rights Considerations

ESG, particularly human rights and modern slavery, has moved beyond voluntary commitments and disclosure. It is increasingly defined by enforceable due diligence, trade restrictions, and regulatory scrutiny across global supply chains.

An estimated 50 million people remain in conditions of modern slavery globally, underscoring both the scale of the issue and the growing regulatory focus on enforcement. Recent reporting in the UK also found that modern slavery cases have reached record levels, highlighting how exploitation continues to evolve across both global supply chains and local labor markets.

A key shift is the move from transparency to accountability. Regulators are no longer asking companies to describe risks. They expect organizations to identify, prevent, and mitigate them, and to demonstrate that they have done so in practice.

From Reporting to Enforcement

Across jurisdictions, a consistent pattern is emerging:

- The EU is advancing mandatory due diligence under the Corporate Sustainability Due Diligence Directive (CSDDD), alongside the Forced Labor Regulation introducing product bans and the ability to investigate and remove goods from the market
- The U.S. continues to expand enforcement through import controls such as the Uyghur Forced Labor Prevention Act, which places the burden of proof on companies to demonstrate goods are not linked to forced labor
- Countries including Canada, Australia, and the UK are increasing expectations around evidence, risk assessment, and accountability, with a clear shift toward risk-based due diligence and stronger enforcement
- Enforcement is expanding beyond individual companies to broader trade and country-level scrutiny, including mechanisms such as Section 301 investigations into forced labor risks

At the same time, enforcement is extending beyond companies to products, supply chains, and even countries—linking human rights risk directly to market access, trade flows, and supply chain continuity.

For organizations with global value chains, human rights risk is no longer primarily reputational. It is a material business risk with direct implications for:

- Market access (import bans, shipment detentions, product restrictions)
- Legal exposure (civil liability, penalties, director accountability)
- Operational resilience (supplier disruption, sourcing constraints)

Regulators increasingly expect companies to look beyond Tier 1 suppliers, identify higher-risk geographies and sectors, and demonstrate ongoing, risk-based due diligence and remediation. In practice, this means organizations must be able not only to identify risk, but to evidence how it is being managed and reduced over time.

CHAPTER 08

Ethical Leadership in an Age of Engineered Volatility

Trust in institutions, including in business, has eroded globally. Now more than ever, business leaders must recognize their responsibility to a wider set of stakeholders. As complexity and volatility build, and enforcement and regulation move in conflicting directions, ethical leadership has never been more important or more commercially valuable.

Consumers are increasingly focused on the employment and environmental impacts of AI and data centers and the relationship between big tech and political leaders. They are watching how companies position themselves, and successful companies will find that ethical conduct is a differentiator in a crowded marketplace.

Workers and consumers have a low tolerance for unethical corporate behavior. Younger generations in particular say purpose at work matters, and many would refuse jobs from, or stop buying from, companies they perceive as unethical. Compliance cannot be a tick-box exercise. It must be an expression of corporate values that stakeholders can hold accountable.

The business case is clear. Analysis from Ethisphere's Ethics Premium report shows that publicly traded companies recognized as the 2026 World's Most Ethical Companies outperformed the broader global market by 8.2 percentage points over a five-year period—reinforcing the link between ethical governance and long-term performance.

Political and policy changes are likely to come in the next several years. Companies that take steps to embed ethical governance and demonstrate genuine accountability today are cementing their reputations and building the credibility that will matter most when political and regulatory winds shift. These companies are engaging in responsible future-proofing.

CHAPTER 09

Building a Resilient Compliance Culture

For compliance managers navigating today's complex landscape, ethical leadership must be reflected in systems that are proactive, flexible, and built to outlast disruption.

Here are five principles for building a third-party risk management program fit for an age of engineered volatility:

1. **Check Your Basics:** Keep frameworks current, ensure clear ownership, and treat beneficial ownership as a baseline requirement, not an advanced capability.

2. **Build for Agility and Flexibility:** Third parties adapt to pressure first. Build modular processes and platforms that can absorb real-time changes in sanctions, trade policy, and export controls.

3. **Enable Integration and Coordination:** Cyber due diligence is a compliance imperative, not an IT issue. AI is accelerating both risk detection and risk creation — deploy it thoughtfully.

4. **Extend Your Ethical Culture Beyond the Enterprise:** Mandatory human rights and environmental due diligence is expanding globally. Embed ethical expectations across your supply chain – don't bolt them on as an afterthought.

5. **Treat Compliance as a Strategic Asset:** Compliance intelligence reveals where risk is accumulating before regulators act. Integrate it into business planning, not just risk management.

CHAPTER 10

The New Imperative

The desire to "get back to normal" is understandable. But in an age of engineered volatility, waiting for stability is itself a risk.

The disruptions reshaping global trade, supply chains, and regulatory frameworks are not temporary. They reflect deeper structural shifts that will define the business environment for years to come. At the same time, social, political, and policy winds can – and likely will – change quickly.

The organizations that thrive won't be those waiting for rules to stabilize. They'll be the ones that lead with their values, embed these values across their supply chains and treat compliance as a strategic asset. In this way, as they adapt to change, these companies will also demonstrate constancy, grounding their business in the ethics needed for long-run success.

In a world where the rules are being rewritten as the game is played, values are the only constant. Lead with them.

About the Authors

VIRNA DI PALMA

Head of Global Content & Brand,
Ethixbase360

Virna brings nearly 20 years of experience in anti-bribery and regulatory compliance, with a multidisciplinary background in international law, counterterrorism, and corporate ethics. As Head of Global Content & Brand at Ethixbase360, she leads the company's thought leadership and strategic brand efforts while advising Fortune 1000 companies on third party due diligence. Her focus includes helping organizations strengthen compliance across global supply and distribution networks by leveraging Tcertification—a globally recognized due diligence standard credited with setting industry benchmarks for third party screening. She also works closely with small and medium-sized enterprises (SMEs) to help them understand and adopt Tcertification as a key component of their compliance programs.

Previously, Virna spent over a decade in a leadership role at a globally respected anti-bribery business association, where she helped shape compliance best practices for multinational corporations and SMEs worldwide. Earlier in her career, she served as Senior Program Director at the American Conference Institute, where she launched the first anti-corruption conferences in Brazil, India, Russia, and the UAE. She began her career at the London-based think tank Demos, researching global security and counterterrorism strategies.

Virna holds a bachelor's degree in political science from Northeastern University and a master's degree in international peace and security from King's College London. She is based in New York City.

About the Authors

JAMES SWENSON

Managing Director,
Ethixbase360

James 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—particularly in the pharmaceutical and life sciences sectors—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.

Prior to joining Ethixbase360, James held senior roles at Exiger and Thomson Reuters/World-Check, where he led global research and operations teams focused on enhanced due diligence and compliance risk intelligence. He has worked in the United States, Europe, and Asia, gaining first-hand insight into regional compliance challenges and cross-border risk.

He holds an MBA from Cass Business School in London and an undergraduate degree from the University of Virginia.

About Ethixbase360

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.

Contact Us

 Website  LinkedIn  Mail