ECI Compliance Week

RISK MANAGEMENT

Compliance must counter rising third-party financial crime risks with risk-based, integrated due diligence



by Ruth Prickett
October 13, 2026

Third-party risks around financial crime are accelerating and becoming more complex. Evolving **sanctions rules**, a renewed focus in the EU and UK on **money laundering**, **bribery** and **corruption**, and the UK's **Failure to Prevent Fraud** criminal offense all put the onus on companies to understand exactly who their third parties are, who is behind them, and how they expose them to risk.

Further concerns are emerging as jurisdictions extend their regulations and sanctions over cryptocurrency exchanges, which can be used as a conduit for opaque financing. Geopolitical upheavals, such as President Trump's capture of President Maduro in Venezuela and ongoing wars in Iran and Ukraine, are shifting criminal activity, as gangs identify new routes to channel illicit money.

Katarina Pranjic, investigations and regulatory policy director at LexisNexis Risk Solutions, warned that it is not only regulated financial firms that could be at risk. Compliance teams in any organization with third-party relationships should check their policies relating to, for example, politically exposed persons (PEPs) and sanctions, she said.

They should also not forget internal fraud risks, she added. "The UK's **Failure to Prevent Fraud** law states that companies could be liable for a fraud committed by a third party if it benefits them. Know your customer and know your supplier rules are key."

Integrated, risk-based, and continuous due diligence

Natalia Gindler Corsini, founder at Prae Venire, said compliance teams are evolving their third-party financial crime risk management by moving away from separate, one-time due diligence processes toward a more integrated, risk-based, and continuous approach.

“Instead of assessing anti-money laundering (AML), sanctions, bribery and corruption, fraud, terrorist financing, sanctions evasion, and other financial crimes separately, mature compliance teams bring these risks together to develop a broader and more complete view of the third parties they do business with,” she explained.

Knowing who the third party is isn’t enough. You need to know who ultimately owns or controls it, how it operates, where it does business, how money moves within the relationship, and whether they have connections or activities that could expose the company to financial crime.

Key risks include:

- Money laundering
- Terrorist financing
- Sanctions violations and evasion
- Bribery and corruption involving financial transactions
- Payment and invoice fraud
- Trade-based money laundering
- Tax-related financial crime
- The use of shell companies or hidden ownership structures
- Transactions intended to disguise the origin, destination, ownership, or purpose of funds

Risk-based approaches recognize that different suppliers, distributors, agents, intermediaries, customers, and business partners represent varying levels of financial crime risk, so they need different review processes.

Deeper reviews include “beneficial ownership analysis, sanctions and PEP screening, adverse-media and public-record checks, understanding the third party’s business activities and source of funds when relevant, and looking closely at how payments and transactions are expected to occur,” Gindler Corsini said.

She explained that compliance teams are paying more attention to warning signs such as payments involving unrelated parties, unusual payment destinations, unexplained intermediaries, inconsistent invoices, and unusual pricing. They are also watching for unnecessary complexity in transactions, or structures that make it difficult to understand who is receiving or controlling the money.

“Financial crime risk cannot be properly managed only at onboarding,” she added. “Third parties may become higher risk if, for example, they change ownership or payment patterns shift. Monitoring should continue throughout the business relationship.”

Warning signs should trigger additional due diligence, investigation, escalation, or a fresh risk assessment. Technology and AI are important in this process, but they are not sufficient on their own.

"Companies are investing in tools that combine external information, such as sanctions lists, corporate registries, beneficial ownership information, PEP databases, and adverse media, with internal procurement, ERP [enterprise resource planning], transaction, invoice, and payment data," Gindler Corsini said. These tools help identify hidden relationships between individuals and companies or shell-company structures, and indirect connections to sanctioned parties. They can flag unusual fund movements and suspicious payment patterns.

Financial crime risks are often interconnected, she pointed out. The same shell company, intermediary, payment, or transaction can be connected to money laundering, sanctions evasion, corruption, or fraud.

Exposure

Companies are most exposed to third-party financial crime risks when they lack a complete view of who they are doing business with, rely too heavily on onboarding controls, fail to recognize changes in risk, or have information spread across different parts of the organization, Gindler Corsini said.

Common causes of exposure include:

- Fragmented responsibility and information
- Limited understanding of ownership and control
- A single common risk approach everywhere
- A disproportionate reliance on onboarding
- Insufficient transaction analysis
- Ineffective use of data and technology

Compliance for the future

Compliance should aim for a more integrated, continuous, and intelligence-driven approach to third-party financial crime risk, Gindler Corsini advised.
Technology and AI are important, but companies also need experienced professionals who understand the risks. They must know how to interpret data and recognize when something does not make sense and should be escalated.

Most importantly, compliance must move from reacting to risks to anticipating them, she said.
Understanding geopolitical developments, changes in ownership, new payment methods, emerging

technologies, transaction patterns, and changes in third-party behavior should become part of ongoing financial crime risk management.

© 2026 COMPLIANCE WEEK, INC.POWERED BY NEWSPACK