



PERSPECTIVES

South of the Border Compliance: Enhancing Integrity & Risk Management in Latin American Operations

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

In February 2025, the Trump administration directed a significant shift in the US Department of Justice's (DOJ) enforcement priorities by announcing a 180-day suspension of new actions under the Foreign Corrupt Practices Act (FCPA). This unprecedented [pause](#), framed as a move to restore US competitiveness and safeguard national interests, coincided with a broader pivot toward trying to dismantle cartels and transnational criminal organizations (TCOs), the majority of which are prevalent in Latin America and the Caribbean. Despite the DOJ's pause on FCPA enforcement, state attorneys-general (AG) may fill the enforcement void left by federal authorities (for instance, the state of California has indicated it will continue to pursue FCPA matters under state laws). The [California Attorney-General's recent legal advisory](#) emphasizes that violations of the FCPA remain actionable under California's Unfair Competition Law (UCL), ensuring that improper payments to foreign officials for business purposes are still illegal and subject to state-level enforcement.

However, while the DOJ may be pulling back, enforcement continues elsewhere. Some countries across Latin America and Europe are stepping up anti-corruption efforts, introducing stricter regulations, and increasing investigative cooperation. This means that multinational companies operating across borders now face a more fragmented yet demanding global compliance landscape.

We examine how companies can adapt their compliance strategies to remain effective in this shifting regulatory environment. This is not a call to scale back compliance efforts, but to reprioritize them. Companies must continue to anticipate enforcement risks, strengthen controls, and build programs that are not only resilient today but future-proof.

ADDRESSING DOJ ENFORCEMENT CHANGES

President Donald Trump's Executive Order argues that FCPA enforcement had become "overexpansive and unpredictable" allegedly impeding US foreign policy and

harming American companies' global competitiveness. Concurrently, the DOJ refocused its efforts toward other crimes, especially targeting drug cartels and TCOs. In a directive titled "[Total Elimination of Cartels and TCOs](#)," US Attorney-General Pam Bondi ordered that the DOJ's FCPA Unit prioritize only bribery cases with clear links to cartel or TCO activity.

The US Securities and Exchange Commission (SEC), which enforces the FCPA's civil provisions, is not directly bound by the DOJ's pause. The White House's directives did not explicitly restrict SEC action, and the SEC retains independent authority over corporate books-and-records and internal controls violations. Still, it is anticipated the SEC will slow-roll new FCPA investigations and coordinate with DOJ's reprioritization, focusing its enforcement on other areas. That said, companies should remember the SEC can still pursue accounting violations stemming from bribery (e.g. false books or inadequate controls), even if the DOJ is less active.

These US shifts are unfolding against a backdrop of intensified anti-corruption efforts globally. The pause in DOJ's FCPA enforcement is unique, most other jurisdictions continue to ramp up anti-bribery enforcement and expect companies to comply with high standards. Latin America in particular has seen a wave of reforms. Over the past years, countries like Brazil, Argentina, Mexico, Peru, Chile, and Colombia have enacted tougher anti-bribery statutes and corporate liability regimes and have collaborated with US investigators on landmark cases. Latin American prosecutors and regulators also are stepping up. For example, Colombia now requires by law business ethics programs and compliance officers to prevent risks of corruption, money laundering and financing of terrorism. Peru offers huge reductions in penalties to companies with compliance programs, and other countries reward robust compliance programs by mitigating or even exempting corporate penalties. In short, while the US temporarily eases off anti-corruption enforcement, foreign authorities are increasing it.

Therefore, multinational companies should not be complacent about the DOJ's pause on the FCPA. The pause *does not decriminalize bribery*, the FCPA remains in force and has a statute of limitations of five years from the date of the alleged offense. Any illicit conduct

during this window could be prosecuted years later (by a future DOJ or by the SEC or foreign regulators). Moreover, the pause is explicitly temporary, DOJ could resume enforcement with revised (possibly more selective) guidelines.

Meanwhile, the pivot to cartel and TCO crime means companies face new risks of enforcement in those domains. For instance, a company that previously might have been investigated under the FCPA for paying bribes in Latin America could now instead face an investigation for “material support” of a terrorist organization if those payments aided a cartel designated as a Foreign Terrorist Organization (FTO).

That said, a presumptive drop in US prosecutions does not equal a decrease of risk. Companies that respond by relaxing controls would be shortsighted; the smarter approach is to treat this period as an opportunity to reinforce compliance efforts, address lingering red flags, and prepare for the eventual resumption of aggressive enforcement.

PREVENTIVE MEASURES: INTEGRITY DUE DILIGENCE AND RISK ASSESSMENTS

In today’s evolving risk landscape, it is critical for companies, especially those operating in Latin America and other high-risk jurisdictions, to implement preventive compliance measures.

Integrity due diligence and comprehensive risk assessments are two outstanding tools to help companies proactively identify who they are dealing with, where their exposures lie, and how to mitigate potential risks before problems arise.

Integrity due diligence involves thoroughly vetting business partners, third-party intermediaries, acquisition targets, and any other affiliates for any integrity-related red flags. This process aims to uncover links to corruption, criminal organizations, sanctioned entities, or other ethical risks that could impact the company. Under the current regulatory landscape, verifying a

partner’s actual beneficial owners is essential, including checking for any politically exposed persons among their ranks and investigating any history of bribery, fraud, money laundering, or litigation.

In high-risk regions, like, for example, Mexico, due to the presence of multiple and fragmented cartels, integrity due diligence can explore connections to cartels, their members, terrorist financiers, or organized crime groups. Conducting local intelligence-gathering activities, such as searching local language media and conducting discreet inquiries, may be necessary, as public records in some countries may be limited. For instance, corporate registries might not disclose actual owners in certain parts of Latin America, and adverse news reports can be unreliable. Therefore, leveraging investigative resources and local expertise is often essential to fully understand a third party’s integrity.

In the current context, leading multinational companies are strengthening their due diligence programs. Some of the best practices for adequate due diligence include:

- **Risk-Based Vetting of Third Parties:** Conducting enhanced background checks on third parties. This may involve reviewing corporate records, litigation history, sanctions screenings, and open-source media entries for each partner. Companies should give special attention to partners in industries or countries with known cartels or widespread corruption activity and conduct periodic updates of the checks.
- **Identify Beneficial Owners and Politically Exposed Persons (PEPs):** Always determine who ultimately owns and controls your intermediaries or joint venture partners. Identify if any owner, director, or key employee is a government official, has familial ties to a PEP, or is linked to criminal networks. Hidden ownership by a crime syndicate or an official’s relative poses significant corruption risks.
- **Leverage Local Intelligence:** In jurisdictions with sparse public data, such as Latin America and the Caribbean, engage reputable advisors to gather reputation information and check for unofficial warning signs (e.g., rumors of payoffs or cartel “protection” arrangements).

- **Integrate Screening for Sanctions Links:** Given that cartels may have FTO designations in key jurisdictions, incorporate checks against [US sanctions lists](#) issued by the Office of Foreign Assets Control (OFAC) and global terrorism lists for all counterparties. Doing business with a designated entity (even indirectly) could result in severe penalties beyond the scope of the FCPA. Enhance customer and partner onboarding processes to include these screenings and document the results.
- **Continuous Monitoring and Updating:** Treat due diligence as an ongoing process rather than a one-time check. Risk profiles can change. For instance, a local partner might develop corrupt relationships over time or be investigated by local authorities. Periodically refresh due diligence for long-term partners and update risk assessments annually (or more frequently for volatile areas). It is also crucial to remain informed about geopolitical developments (e.g., a new anti-corruption law in a country or a city becoming a hotspot for cartel activity) and adjust your due diligence scope accordingly.
- **Transaction Monitoring Algorithms:** Companies should deploy rule-based and machine-learning algorithms across financial operations to flag suspicious transactions. These tools can detect red flags such as abnormally large or round-numbered payments, payments just below approval thresholds, and transfers to high-risk jurisdictions unrelated to legitimate business. Modern systems reduce false positives by learning context-specific patterns of normal behavior, enabling compliance teams to focus on genuine risks.
- **Graph Analytics for Network Links:** Graph analysis uncovers hidden connections between entities and individuals such as a shared intermediary between a third-party agent and a foreign official, or shell companies with a common beneficial owner. These insights are vital in identifying networks used to launder funds or channel bribes, especially when ties to cartels or TCOs are intentionally concealed.
- **Continuous Screening and Optical Character Recognition (OCR):** Automated screening of counterparties and transactions against global sanctions lists, FTO designations, watchlists, and adverse media enables real-time alerts. Integrating OCR and web scraping allows systems to capture newly published red flags, such as media reports linking a vendor to money laundering or criminal investigations, supporting proactive response before regulators intervene.
- **Integrating Know-Your-Customer (KYC) and ERP Data:** Many companies possess valuable compliance-related data that remains siloed. By connecting KYC information with Enterprise Resource Planning (ERP) and procurement systems, inconsistencies can be flagged, such as mismatched vendor addresses, unexpected overlaps between employee and vendor records, or repetitive small payments indicative of invoice fraud or corruption.
- **Tailored Analytics for Industry Risks:** Each sector faces unique financial crime patterns. For example, pharmaceutical firms may need to track high commission payments in regions with systemic corruption in healthcare procurement. Mining companies must monitor whether logistics or

LEVERAGING DATA ANALYTICS

Traditional compliance frameworks are no longer sufficient to manage the rapidly evolving risks. In response to the DOJ's shift in enforcement focus, particularly toward disrupting money laundering channels and support to designated FTOs, data analytics has become indispensable for corporate compliance.

One area where analytics can be a game-changer is in combating money laundering and terrorist financing, which are often intertwined with corruption and organized crime. Sophisticated criminal networks funnel bribe payments or illicit proceeds through complex transactions, but these often leave digital traces. By employing modern data analysis techniques, companies can spot anomalies indicative of wrongdoing. For example:

security payments could be funneled to cartels or militant groups in conflict zones. Tailoring data models to these risks enhances specificity and detection effectiveness.

- **Verified Financial Intelligence (VFI) and Visualization Tools:** Platforms offering interactive dashboards, heat maps, and drill-down capabilities make it easier to investigate and document red flags. By visually mapping out transaction flows and network relationships, compliance officers can better trace illicit patterns and prepare internal investigations or disclosures.

Adopting these data-driven approaches significantly enhances the effectiveness and efficiency of compliance. It allows a shift from reactive to proactive oversight, empowering organizations to detect red flags early, reduce regulatory exposure, and maintain operational integrity, even in high-risk jurisdictions. When implemented well, data analytics can act as a force multiplier for compliance teams, enabling them to supervise sprawling global operations with greater confidence. In an era where illicit transactions can be complex and transnational, and there is increased global scrutiny, data-driven compliance isn't optional, it's a strategic necessity.

ENHANCING CORPORATE CONTROLS: A CHECKLIST

To address these evolving risks and enforcement changes, companies should fortify their internal controls and compliance infrastructure. Below is a checklist of key corporate controls to enhance their capabilities, along with notes on effective implementation:

1) Governance and Oversight

- Clearly define and document governance structure, including relevant committees, roles, responsibilities, and reporting frequency.
- Senior leadership must visibly communicate and reinforce ethical conduct and compliance as fundamental organizational values.
- Ensure the Chief Compliance Officer (CCO) has direct reporting lines to the board or audit committee, guaranteeing independence.

2) Management Information Systems (MIS) Reporting

- Regularly validate the adequacy and accuracy of MIS outputs to inform management effectively on the internal control framework's current state.
- Integrate Know-Your-Customer (KYC) data with internal financial systems for enhanced cross-verification.

3) People, Processes, and Procedures

- Document controls clearly, specifying roles responsible, applicable procedures, and the corresponding technology platforms used.
- Provide regular, targeted training emphasizing practical scenarios involving bribery solicitations, cartel interactions, and compliance with anti-money laundering (AML) policies.

4) Control Inventory

- Maintain a detailed inventory of internal controls, capturing control name, purpose, risk mitigation strategies, control owner, testing frequency, and necessary technology platforms.

5) Integrity Due Diligence (IDD) and Third-Party Management

- Perform thorough vetting of third parties, especially those with governmental interactions or operating in high-risk areas. Identify beneficial ownership, political exposure (PEPs), and links to criminal organizations.
- Ensure contracts explicitly detail anti-corruption commitments, compliance audit rights, and termination clauses for detected misconduct.
- Continuously update due diligence efforts based on changes in geopolitical risks, regional compliance regulations, and new information obtained from local intelligence.

6) Internal Accounting and Financial Controls

- Strengthen financial controls to prevent off-book payments and enforce accurate, transparent record-keeping aligned with FCPA's accounting requirements.
- Implement multi-level approval processes for high-risk transactions and utilize data analytics to detect anomalous financial activities.
- Synchronize financial controls explicitly with risks of indirect funding or transactions linked to cartels or terrorist-designated entities.

7) Data Analytics and Monitoring

- Deploy advanced analytics and artificial intelligence-driven monitoring to detect suspicious transaction patterns and indirect associations with sanctioned entities or criminal organizations.
- Regularly leverage graph analytics tools to reveal complex networks and hidden relationships among entities and individuals that might indicate corruption, fraud, or money laundering.

8) Reporting Mechanisms and Crisis Management

- Establish secure, confidential reporting channels enabling employees and partners to report compliance concerns without fear of retaliation.
- Implement clear crisis response protocols, outlining steps for evidence preservation, investigation initiation, self-disclosure considerations (even with DOJ's current stance, self-disclosure to the SEC or foreign regulators might still be advisable in certain scenarios), and remedial actions.

9) Implementation and Continuous Improvement

- Assign clear accountability for each control measure to specific roles within the organization.
- Set measurable compliance objectives with defined timelines and routinely track progress through internal audits or external compliance reviews.
- Foster an agile compliance environment, regularly updating controls and training programs in response to shifting global regulatory landscapes and emerging threats.

Each of these control enhancements should be implemented with tangible commitment and oversight. It's not enough to have a paper checklist – **effective implementation** is key. Companies may consider engaging external experts or auditors to test their controls' effectiveness periodically. An external compliance review can provide assurance that the checklist measures aren't just in theory but are working in practice. By systematically enhancing these corporate controls, companies create a robust shield against both current and future risks.

STRENGTHENING RISK MANAGEMENT STRATEGIES

The final piece of the puzzle is ensuring that a company's risk management and compliance strategy is built to last, resilient against the flow of political leadership and enforcement priorities. History shows that DOJ and SEC focus areas can shift with each administration. Today it's cartels; tomorrow it could swing back to corporate fraud or sanctions or a new threat altogether. To navigate this uncertainty, companies should adopt a long-term, principles-based approach to compliance that doesn't rely solely on the priorities of the moment.

First and foremost, continue investing in compliance as a long-term asset. Companies that maintained strong compliance programs through past lax enforcement periods have consistently fared better when crackdowns resume. Conversely, if a company were to disband parts of its compliance program during the FCPA pause, it would find itself scrambling (and exposed) later. A long-term view accepts that enforcement is cyclical, and the cost of rebuilding compliance (or the legal fallout of compliance failures) far outweighs the cost of maintaining it steadily.

On the other hand, develop a holistic risk management strategy that encompasses not just anti-bribery, but adjacent risk areas like sanctions, AML, fraud, and human rights. This integrated approach is increasingly necessary, for example, a bribe may trigger accounting fraud (books and records violations) and money laundering issues simultaneously. If your program covers all these bases, it will remain robust no matter which law enforcers decide to target. The current US focus on TCOs illustrates this, a company might avoid FCPA trouble but still get hit for sanctions or AML violations if it isn't monitoring those risks. A unified compliance framework breaks down silos and allows the company to respond cohesively to any form of misconduct. Many leading companies are moving in this direction, aligning their anti-corruption, AML, and even Environmental, Social, and Governance (ESG) efforts under a common risk governance model. This also future proofs the organization for emerging regulatory trends.

Another key strategy is staying informed and agile regarding legal developments worldwide. Companies should actively monitor not only US policy changes but also enforcement news and legislative reforms in the countries where they operate. As we see, Latin America is strengthening its own enforcement and compliance expectations. Europe, Asia, and Africa likewise have evolving anti-corruption regimes. By keeping a finger on the pulse of these changes, a company can anticipate shifts. An agile compliance function will update policies and training quickly in response to new laws or risks.

It is crucial to embed a strong ethical culture and internal accountability that transcends specific laws. A workforce that is committed to integrity because it's the right thing to do, not just out of fear of enforcement – will carry that ethos through regardless of external changes. If employees see that the company truly cares about ethical conduct in good times and bad, they will be less likely to cut corners even if they perceive enforcement is lax. Culture is often cited by enforcement agencies when deciding whether to bring charges or give credit. A demonstrably strong culture can be a company's best defense.

Finally, consider that effective risk management in uncertain times may benefit from external perspectives. Engaging independent monitors or advisors periodically to review your program can provide assurance that you haven't developed blind spots. Peer benchmarking within your industry is also useful. For instance, some companies might share strategies on handling increased solicitation for bribes by local officials in the absence of US enforcement. Learning from each other can be invaluable.

While the Trump administration's enforcement priorities mark a significant shift, they are by no means a signal for multinationals to relax their guard. If anything, the complexity of the current environment (US reprioritization versus global ramp-up) demands a more nuanced and resilient compliance approach. Companies should take a broad, long-term view: doubling down on ethical practices now will keep them on solid footing regardless of whether the next few years bring a continued lull or a resurgence of anti-corruption enforcement. By implementing rigorous preventive measures, leveraging technology, fortifying internal controls, and fostering

an enduring culture of compliance, organizations will not only weather the present storm of change but emerge stronger and better prepared for whatever comes next.

CONCLUSION

The DOJ's pause on FCPA enforcement and its sharpened focus on cartels and transnational crime mark a critical inflection point for global businesses. As discussed throughout this article, while US enforcement may appear to recede temporarily, the risks associated with corruption, financial crime, and regulatory scrutiny remain high, and in many cases, are shifting jurisdictions rather than disappearing.

In this evolving context, companies must remain proactive and strategic. Strengthening compliance programs, enhancing internal controls, leveraging data analytics, and fostering an enduring culture of ethics are all essential actions. The FCPA pause should not be seen as a relaxation of accountability, but rather as an opportunity to prepare for a likely return to enforcement.

External consultants can help companies stay ahead of regulatory changes and mitigate risk effectively through the following:

- **Enhanced due diligence investigations** focused on identifying integrity risks, hidden ownership, and links to organized crime.
- **Corporate risk assessments** tailored to evaluate exposure to bribery, money laundering, and sanctions violations.
- **Development and optimization of compliance programs**, aligned with global standards and local regulatory requirements.
- **Forensic and data analytics tools** to uncover suspicious patterns, illicit networks, and transaction anomalies.
- **Implementation of anti-money laundering (AML) safeguards** in high-risk sectors.

The goal is not to retreat; it's to move forward strategically.

ACKNOWLEDGMENTS

We would like to thank our colleagues, Karyl Van Tassel, Carlos Mahecha, Mariano de Alba, Ken Feinstein, and Anne Walton for their insights and expertise that greatly assisted this research.

MORE ABOUT J.S. HELD'S CONTRIBUTORS

[Ken Feinstein](#) is a Senior Managing Director in the [Digital Investigations and Discovery Service Line](#) within the [Global Investigations practice](#) at J.S. Held. Based in J.S. Held's New York City office, Ken specializes in investigative data analytics and provides investigations, regulatory risk and litigation support solutions spanning multiple sectors, including retail and consumer products, life sciences, technology, financial services, industrial products, and government agencies. His clients include law firms and Fortune 500 legal and compliance teams for whom he delivers large scale, complex investigations, regulatory response matters, proactive anti-fraud efforts, and compliance programs. He is a member of the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

Ken can be reached at ken.feinstein@jsheld.com or +1 917 277 7868.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

J.S. Held, its affiliates and subsidiaries are not certified public accounting firm(s) and do not provide audit, attest, or any other public accounting services. J.S. Held is not a law firm and does not provide legal advice. Securities offered through PM Securities, LLC, d/b/a Phoenix IB or Ocean Tomo Investments, a part of J.S. Held, member FINRA/SIPC. All rights reserved.