Oversight

WHITE PAPER

Beyond Periodic Audits: Why Continuous FCPA Compliance Requires Finance Risk Intelligence

Examining the Impact of the Foreign Corrupt Practices Act

Author: Asim Farooqi

Executive Summary

Traditional anti-corruption programs rely on periodic audits, sampling, and manual review. This model is insufficient for modern transaction volumes, third-party networks, and the speed at which corruption risk hides inside ordinary financial activity.

The enforcement landscape is shifting. U.S. FCPA enforcement has narrowed its focus to national security and economic competitiveness priorities, while European regulators are broadening their reach with aggressive new frameworks.

Three data points frame the challenge:

- Roughly 90% of FCPA enforcement matters involve third-party intermediaries.[2]
- The EU Anti-Corruption Directive sets fines of at least 5% of worldwide turnover.[1]
- The compliance software market is projected to exceed $74 billion by 2031.[3]

This white paper argues that continuous, AI-enabled Finance Risk Intelligence represents the new compliance operating model: one that moves from periodic sampling to always-on detection, prioritization, and governed action.

Why the Traditional Compliance Model Is Breaking

Most corporate anti-corruption programs were designed for a different era. They rely on periodic audits conducted quarterly or annually, manual sampling of a small fraction of transactions, static rules-based screening that flags only the most obvious patterns, and retrospective investigations triggered by whistleblowers or external events.

This approach made sense when transaction volumes were lower, third-party networks were simpler, and regulators accepted good-faith effort as sufficient. None of those conditions hold today.

Modern enterprises process millions of transactions across dozens of countries, through hundreds or thousands of third-party relationships. Bribery does not announce itself. It hides inside ordinary-looking expenses, invoices, and payments:

- Gifts or entertainment involving government-connected parties
- Vague consulting or marketing invoices without clear deliverables
- Duplicate or inflated reimbursements
- Split transactions structured to stay below approval thresholds
- Unusual commissions or rebates to intermediaries
- Payments to high-risk jurisdictions without clear business justification
- Payments routed to mismatched bank accounts or entities
- Repeated anomalies involving the same employee, vendor, or intermediary
- Approval and documentation irregularities

A periodic audit that samples 2-5% of transactions will miss most of these signals. By the time a pattern is identified, the exposure may span years and millions of dollars.

© 2026 Oversight. All rights reserved.

The Enforcement Landscape Is Changing, but the Control Imperative Is Not

In early 2025, the Department of Justice paused new FCPA investigations. By June 2025, new guidelines refocused enforcement on cases involving national security threats, economic competitiveness, cartels and transnational criminal organizations, shell companies and money laundering, and state-owned enterprises.[4]

This does not mean FCPA enforcement has ended:

- The SEC retains independent authority to bring civil actions under the accounting provisions
- Whistleblower programs continue to generate leads[5]
- Books-and-records requirements remain fully in force
- DOJ preserved its ability to pursue egregious conduct and recidivists

Meanwhile, Europe is moving in the opposite direction. The EU Anti-Corruption Directive (effective May 2026) sets corporate fines of at least 5% of worldwide turnover.[1] The UK Economic Crime and Corporate Transparency Act introduced a failure-to-prevent-fraud offence in September 2025.[6] France's Sapin II continues to require compliance programs.

Recent enforcement examples underscore the stakes:

- Millicom/TIGO Guatemala: $118M+ resolution for bribing legislators through intermediaries[7]
- RTX/Raytheon: ~$950M across multiple jurisdictions
- Gunvor: $660M+ for bribery to secure oil contracts in Africa
- SAP: $220M+ for third-party bribery schemes
- Airbus: $3.9B global resolution

The common thread: third-party intermediaries, payments disguised as legitimate expenses, and books-and-records failures that allowed schemes to persist undetected.[8]

© 2026 Oversight. All rights reserved.

Finance Risk Intelligence as the New Compliance Operating Model

Finance Risk Intelligence is not a feature or a product category. It is an operating model for how finance and compliance teams identify, prioritize, and act on corruption risk continuously rather than periodically.

The model has six core capabilities:

1. Continuous Risk Identification
Monitor all transactions, not samples. Apply AI and machine learning to score risk at the transaction level across expense reports, invoices, P-card spend, and vendor payments.

2. Signal Connection
Link weak signals across data sources. A single anomaly may be benign; a cluster of related anomalies across multiple systems reveals a pattern.

3. Risk Prioritization
Score and rank findings so investigators focus on the highest-risk items first, not the most recent or most visible.

4. Efficient Investigation
Provide context, evidence, and audit trails that reduce investigation time from weeks to hours.

5. Governed Action and Documentation
Connect detection to resolution through defined workflows, human oversight, and traceable decision records.

6. Feedback Into Policies and Controls
Use findings to strengthen rules, update risk models, and close gaps, creating a system that improves over time.

This model replaces the periodic audit cycle with a continuous loop: detect, prioritize, investigate, act, measure, improve.

© 2026 Oversight. All rights reserved.

FCPA Risk Hides Inside Everyday Financial Activity

The FCPA has two main components. The anti-bribery provisions prohibit payments to foreign officials to obtain or retain business. The accounting provisions require accurate books and records and adequate internal controls.[9]

Critically, a company can violate the FCPA solely through inaccurate books and records, even if no bribe occurred. This makes the accounting provisions the broader compliance obligation.[2]

Bribes are rarely labeled as bribes. They are disguised as ordinary business expenses:[10]

- Consulting fees paid to intermediaries with no clear deliverables
- Commissions or rebates to agents in high-risk jurisdictions
- Travel and entertainment expenses involving government officials
- Vendor payments routed through shell companies
- Inflated invoices where the excess funds bribes[11]
- Miscellaneous expenses that avoid categorization

The challenge is that each of these looks like a normal payment in isolation. The corrupt intent only becomes visible when you examine patterns across thousands of transactions: the same vendor receiving vague invoices quarter after quarter, payments clustering around government decision dates, amounts structured just below approval thresholds.

This is why sampling fails. Corruption hides in the volume. Only continuous, transaction-level monitoring can surface the patterns that periodic reviews miss.[12]

© 2026 Oversight. All rights reserved.

How AI Helps Identify and Prioritize Meaningful Risk

AI does not determine whether bribery occurred. That judgment belongs to trained investigators and legal counsel. What AI does is review every transaction, weigh multiple weak signals simultaneously, and surface the items most likely to represent meaningful risk.

A well-designed AI system for FCPA compliance:

- Analyzes 100% of transactions rather than sampling a fraction
- Scores risk based on multiple factors weighted together
- Identifies clusters of related anomalies across data sources
- Learns from investigator feedback to improve over time
- Provides transparent, explainable scoring so reviewers understand why an item was flagged
- Maintains human oversight at every decision point

The key distinction is between detection and determination. AI detects patterns that warrant investigation. Humans determine whether those patterns represent actual violations.

This division of labor is critical for regulatory credibility. Regulators expect companies to demonstrate that their AI systems are explainable, that scoring logic can be articulated, and that human judgment governs all consequential decisions.[12] Black-box models that flag transactions without explanation do not satisfy the DOJ's Evaluation of Corporate Compliance Programs or equivalent standards in other jurisdictions.

The practical benefit is efficiency. Instead of investigators spending weeks reviewing random samples, they focus immediately on the highest-risk items with full context and evidence already assembled.

© 2026 Oversight. All rights reserved.

Where Continuous Monitoring Creates the Most Value

Third Parties and Intermediaries
Roughly 90% of FCPA enforcement matters involve third-party intermediaries.[2] Continuous monitoring of agent fees, consultant payments, distributor commissions, and joint-venture disbursements surfaces risk that periodic due diligence reviews miss.[11]

High-Risk Markets and Government Touchpoints
Transactions involving government-connected counterparties, state-owned enterprises, or jurisdictions with high corruption indices require heightened scrutiny.[13] AI can flag these automatically based on entity attributes and payment patterns.

Mergers and Acquisitions
Pre-acquisition transaction analysis can reveal corruption exposure before closing. Post-acquisition monitoring ensures inherited risks are identified and remediated promptly, supporting DOJ's safe harbor expectations.[14]

Cross-Border Corruption, Sanctions, and Money Laundering
Bribery, money laundering, and sanctions evasion use the same mechanisms: shell companies, layered transactions, and mischaracterized payments.[15] Integrated monitoring across these risk domains surfaces connections that siloed compliance functions miss.

A single payment to a government-connected intermediary may simultaneously trigger FCPA anti-bribery violations, books-and-records failures, AML reporting obligations, and sanctions violations if the official or entity is designated.

© 2026 Oversight. All rights reserved.

Sector Spotlight: Where Exposure Concentrates

Certain industries face heightened FCPA risk due to their reliance on government contracts, permits, or regulated markets:

- Energy and extractives (concessions, exploration permits)
- Aerospace and defense (government procurement)
- Healthcare and life sciences (state-run hospitals, drug approvals)
- Telecommunications (spectrum licenses, infrastructure permits)
- Financial services (sovereign wealth fund relationships)
- Construction and infrastructure (public works contracts)

Companies in these sectors typically operate through complex webs of local agents, joint-venture partners, and government-facing intermediaries. The combination of high-value contracts, opaque regulatory processes, and reliance on third parties creates conditions where corrupt payments can flourish undetected without robust transaction-level monitoring.

Enforcement data confirms this concentration. Energy, defense, and healthcare companies account for a disproportionate share of FCPA resolutions by dollar value. Companies in these sectors should apply enhanced due diligence to all government-facing relationships and implement continuous monitoring of payment patterns to high-risk jurisdictions.

© 2026 Oversight. All rights reserved.

How Companies Should Respond

Regulators worldwide have converged on a common expectation: compliance programs must be effective in practice, not merely designed on paper. The DOJ's Evaluation of Corporate Compliance Programs, the UK Bribery Act's adequate procedures defense, and the EU Directive's mitigation provisions all reward companies that can demonstrate their controls work.[12]

A modern anti-corruption compliance program should include:

- Continuous transaction monitoring across all payment channels
- AI/ML-driven anomaly detection that scores risk at the transaction level
- Risk-tiered third-party due diligence with ongoing screening
- Automated red-flag identification across expense, invoice, and P-card data
- Audit-ready evidence that demonstrates controls operated effectively
- Integration of anti-corruption, AML, and sanctions monitoring
- Regular training calibrated to role-specific risk exposure

The Economics: Program Cost Versus the Cost of a Violation

The business case for investment in compliance technology is straightforward. Recent FCPA resolutions have ranged from $118 million to $950 million, exclusive of legal fees, remediation costs, and reputational damage.[7] By contrast, compliance software and monitoring platforms represent a fraction of that exposure.

The compliance software market is projected to exceed $74 billion by 2031, reflecting broad enterprise recognition that manual, periodic compliance reviews are insufficient for the speed and complexity of modern global operations.[3]

Companies that invest in continuous, data-driven monitoring gain three advantages:

1. Earlier detection, which limits the scope and duration of violations
2. Demonstrable compliance effort, which supports cooperation credit[7]
3. Operational efficiency, reducing the cost of compliance per transaction

© 2026 Oversight. All rights reserved.

Looking Ahead: Where Anti-Corruption Compliance Is Going

Several trends will shape anti-corruption compliance over the next three to five years:

- Multi-jurisdictional enforcement will become the norm, not the exception
- Regulators will expect real-time or near-real-time monitoring capabilities[12]
- AI-driven compliance tools will shift from competitive advantage to baseline expectation
- Data-sharing between enforcement agencies will accelerate cross-border investigations
- Whistleblower programs will shorten the time between misconduct and discovery[5]

Companies that build robust, technology-enabled compliance programs today will be positioned to meet these evolving expectations. Those that rely on periodic manual reviews and reactive investigations face growing exposure as enforcement becomes faster, more coordinated, and more data-driven.

Oversight's Finance Risk Intelligence Platform helps organizations meet this moment by applying AI and machine learning to transaction-level data, scoring FCPA risk, flagging mischaracterized expenses, surfacing third-party anomalies, and generating audit-ready evidence that demonstrates controls are operating effectively.

© 2026 Oversight. All rights reserved.

References

1. New FCPA Guidance Released by the DOJ and SEC, Westlaw Practical Law

2. How to Create a Community Resource Guide, TechSoup

3. AfIn Compliance Bulletin, Alliance for Integrity

4. Defending an FCPA Books and Records Violation, Willkie Farr & Gallagher, New York Law Journal (January 24, 2013)

5. Checklist for International Business Contracts, HMT Law

6. What Is the Difference Between a Grease Payment and a Bribe?, Hilder & Associates

7. Association of Certified Fraud Examiners (ACFE)

8. FCPA Accounting Provisions, White Collar Attorney

9. U.S. Department of Justice, Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (June 2025)

10. DLA Piper, FCPA Year in Review: Enforcement Trends and What's Ahead in 2026 (January 2026)

11. EU Directive 2026/1021 on Combating Corruption (in force 31 May 2026), European Commission, EU Legislation on Anti-Corruption

12. UK Economic Crime and Corporate Transparency Act 2023; Failure to Prevent Fraud Offence (in force 1 September 2025)

13. U.S. Department of Justice, TIGO Guatemala Paid Over $118M to Resolve Foreign Bribery Investigation (November 2025)

© 2026 Oversight. All rights reserved.

References (continued)

14. Foley Hoag, Anticorruption Enforcement and the FCPA: 2026 Year in Preview (January 2026)

15. Mordor Intelligence, Compliance Software Market Size & Share Outlook to 2031 (2026)

16. Dataintelo, Anti-Bribery and Corruption Compliance Market Research Report 2033 (2025)

17. Mordor Intelligence, Governance, Risk, and Compliance (GRC) Software Market Report 2026-2031

18. U.S. Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs

19. OECD, Generative AI for Anti-Corruption and Integrity in Government (Working Paper)

20. International Bar Association, How AI Can Reshape Anti-Corruption Compliance

21. Third-Party Intermediaries in FCPA Enforcement Actions, Foreign Corrupt Practices Act Clearinghouse, Stanford Law School; White & Case, Global Compliance Risk Benchmarking Survey: Third-Party Management

22. Volkov Law Group, FCPA Compliance Lessons from 2025 (Part II): Why Reduced Enforcement Activity Does Not Reduce Risk (February 2026)

23. U.S. Department of Justice, Safe Harbor Policy for Voluntary Self-Disclosures Made in Connection with Mergers and Acquisitions (October 2023)

24. LexisNexis Risk Solutions, True Cost of Financial Crime Compliance Global Study (financial institutions, $206.1 billion)

25. Ankura, The Extended Network: Managing Third Parties' Bribery Risks (December 2025)

26. Paul, Weiss, FCPA Enforcement and Anti-Corruption Developments: 2025 Year in Review (January 2026)

© 2026 Oversight. All rights reserved.