Data Analytics for Anti-Corruption Compliance

Lextegrity

The Problem

Preventing and detecting corruption as well as fraud, sanctions violations, and other non-compliance is of paramount importance to most global organizations. However, it can be extremely difficult when risks may exist in millions of financial transactions and finding instances of non-compliance may be more like finding a needle in a haystack. At the same time, enforcement agencies have imposed heightened standards that define an effective compliance program as one that can detect corruption and other non-compliance immediately and ensure that non-compliance does not become systemic within an organization.

These facts have led many compliance organizations to realize that relying on whistleblower reports or sample-based auditing and monitoring is a necessary, but insufficient, way to prevent and detect corruption in real-time. Organizations have instead focused on real-time transactional monitoring using data analytics to detect fraud or corruption-related financial transactions and prevent wrongdoing from becoming systemic. In today's increasingly complex business environment, a robust and data-driven compliance program is essential to mitigating corruption risks and adhering to regulations like the U.S. Foreign Corrupt Practices Act (FCPA), UK Bribery Act or Sapin II in France.

The Solution

Compliance monitoring systems can identify suspicious transactions by continuously reviewing the financial transactions of companies and individuals. These systems can analyze historical and real-time data to recognize patterns or outliers that indicate fraud, corruption, or other illegal activities. Forensic accountants and other compliance stakeholders can expedite their investigations and make more informed decisions by implementing a compliance monitoring system.

Every company will have unique risks; therefore, it's crucial to have processes and solutions in place that are iterative, and that can evolve and adapt as your risk profile changes, and take a minimal amount of technical skill or data analytics expertise to set up and maintain.

Here are typical schemes and three example analytics that can help detect each one:

Consulting / Professional Services Contracts:

- Large or unusual payments made to a consultant
    - » Analytics can include a combination of payment type, statistical anomaly detection, and aggregate analytics

- Unusual or inconsistent fee structures, such as consulting fees structured in a way that appears to hide the true nature of the payment
    - » Analytics looking at high-risk general ledgers, keyword analysis, payments made using usual payment methods

- High-risk third party without due diligence or change in scope after due diligence
    - » Analytics could include monitoring those transactions immediately after onboarding or creating custom analytics to monitor specific high-risk transactions from the consultant (for example, lobbying and licensing assistance)

Sales Commissions:

- High commission rates compared to peers
    - » The analytics here are self-explanatory, looking at anomalies compared to other sales intermediaries; the key is getting the correct data

- Commissions paid to individuals or entities with no apparent role in the sales process
    - » Analyze key words or patterns associated with transactions that may suggest inappropriate activity
    - » Identify outliers in commission amounts, payment patterns, and payment frequencies compared to the typical patterns observed in the organization

- Commission payments unrelated to specific sales or revenue targets
    - » Develop custom risk analytics with a model based on multiple factors, such as commission amount, recipient type, responsible department, Purchase Order type and payment type, to identify high-risk commission payments that warrant further investigation

Intermediary Transactions:

- Complex transaction structures involving multiple parties or jurisdictions
  - » Analytics that involve bill-to, ship-to, pay-to countries

- Unusual payment terms or payment routes
  - » Analytics looking at expedited transactions, keyword analysis

- Transactions with offshore entities or jurisdictions known for bank secrecy or lack of regulation
  - » Analytics looking at high-risk countries and mismatches between vendor country details and payment/bank country details

Data for Anti-Corruption Analytics and Monitoring

Anti-corruption analytics and monitoring for corporations typically involves collecting and analyzing various types of data to identify potential risks and instances of corruption. Relevant types of data include:

Financial data: This includes financial statements, accounting records, and transactional data used to identify suspicious behavior patterns, such as large, unexplained payments to third parties or discrepancies in financial reporting.

Employee data: Employee data can help identify potential conflicts of interest, such as employees with close ties to vendors or customers or employees with access to sensitive information who may be vulnerable to bribes or other forms of corruption.

Vendor data: Information on vendors and suppliers can help identify potential risks, such as vendors with a history of corruption or those closely tied to government officials.

Compliance data: Compliance data includes information on policies, procedures, and training programs related to anti-corruption efforts. Monitoring compliance data ensures that compliance teams are implementing programs effectively. Pre-approval data can also be used to validate approvals against actual payments.

Public data: Publicly available data, such as news articles, government reports, and social media activity, can help identify potential risks and instances of corruption that other data sources may not capture.

The Results

By embracing a data-driven approach to compliance, organizations can detect potential violations more efficiently and proactively prevent corruption risks before they escalate. Harnessing the power of data creates a more transparent and accountable business environment.

As the compliance landscape becomes increasingly complex, compliance professionals must leverage the most advanced technology and tools to stay ahead of sophisticated offenders. By utilizing compliance monitoring systems in their monitoring and investigations, stakeholders can expedite their efforts, reveal hidden risks and potential schemes, and contribute to more robust and effective compliance programs.

About Lextegrity

Lextegrity provides innovative enterprise data analytics and automation technology for compliance and audit professionals at leading global companies. This first-of-its-kind software is created by former in-house compliance and audit professionals who have operationalized compliance and audit programs globally. Organizations use our software suite to prevent and detect risks related to fraud, corruption, sanctions, kickbacks, and conflicts of interest. Our software unifies compliance systems and manages risk across the spend lifecycle for an end-to-end view in real-time.

Lextegrity's software has been before enforcement agencies globally in 12 separate company engagements and was even cited by the SEC as a remediation factor in a client's FCPA resolution. It has been chosen by several companies after the appointment of compliance monitors or after the start of an investigation and has been a factor in resolving those matters, including helping to secure a DOJ declination.

To learn more about how Lextegrity can digitally transform your compliance program, visit Lextegrity.com or email info@lextegrity.com.

Lextegrity