Applying Data Analytics
and
Periodic Monitoring to Compliance

A Forensic Protocol for Mitigating Risk,
Reducing Regulatory Exposure,
and
Measuring the Efficacy of Compliance Programs

By

Jeffrey Harfenist

February 2022

I. It's Not a Question of If

It is no longer a question of whether your compliance function should be integrating data analytics into your monitoring program, but to what extent. There are countless reasons to incorporate data analytics into your compliance protocols, including, but not limited to the following:

- The SEC and DOJ are expecting the compliance function to integrate some form of analytics into their monitoring, testing, and remediation efforts.
- Early detection of wrongdoing is critical to reducing the myriad of potential costs (i.e., fines, disgorgement, investigations, litigation) associated with non-compliance.
- Data analytics tools that are properly focused can be very effective and can also provide a host of ancillary benefits outside the fraud arena.
- The sizeable bounties earned by whistleblowers has had the unintended effect of placing companies in a race with their employees to uncover wrongdoing.

This paper outlines a protocol for applying data analytics and periodic monitoring to assist boards, general counsel, compliance professionals and external counsel in mitigating risk, reducing exposure, and measuring the efficacy of an organization's compliance programs.

II. What is a Monitoring Program

As depicted in ***Figure 1*** below, a monitoring program integrates sound forensic practices with data analytics to timely detect undisclosed conflicts of interest, non-economic transactions, internal control and/or compliance failures, and potentially collusive behaviors.

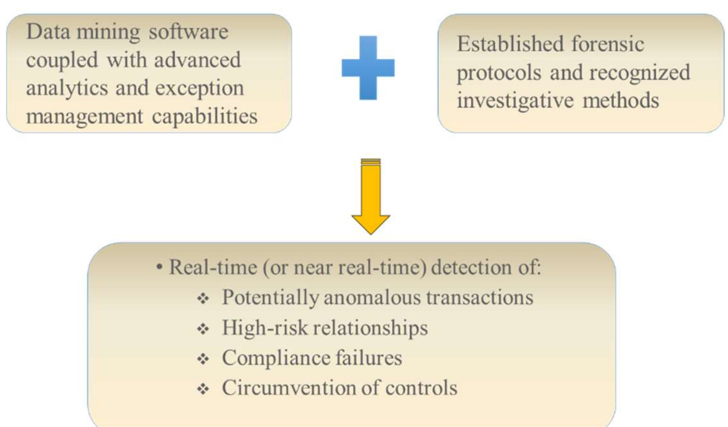


Figure 1

Unlike traditional sampling techniques that analyze a small fraction of transactions drawn from a much larger data set, monitoring applications examine 100 percent of the population of transactions, leading to substantially greater coverage and a commensurate reduction in risk.

Monitoring systems can identify prohibited transactions and potentially illegal behaviors in a company's global business by testing for data inconsistencies, suspicious trends, inconsistent relationships, policy violations, missing data, and a host of other high-risk attributes associated with fraud. These tests can be performed remotely, and based upon the results, the appropriate personnel can be routed to those locations posing the greatest risk of loss and exposure. This approach produces increased efficiency, reduces travel costs, and allows companies to focus finite resources on their highest and best use – in effect, allowing companies to do more with less.

III. Monitoring Provides a Risk Mitigation Solution

Investigating potentially fraudulent practices is labor intensive and inefficient in the absence of a qualified engagement team, and the thoughtful application of forensic tools by skilled experts. As a result of the complex relationships that exist between a company's operations and its control environment, the investigative process needs to be iterative. The approach depicted in ***Figure 2*** involves procedures being conducted in successive phases that build on the results of previous analyses and the results obtained. Consider applying this protocol in the context of conducting a proactive risk and compliance review intended to test the effectiveness of an entity's compliance program. With some limited exceptions (conducting in-person interviews), each of the actions in ***Figure 2*** could be conducted, in whole or in part, using data analytics and monitoring. For example, consider the process of performing an entity-level risk assessment across a global organization. Putting aside the more elementary anti-corruption risk factors typically considered, such as conducting operations in countries with a known culture of corruption, or the use of sales agents and other third-party intermediaries, a monitoring solution can identify other attributes possessing a high indicia of fraud. These would include transactions that:

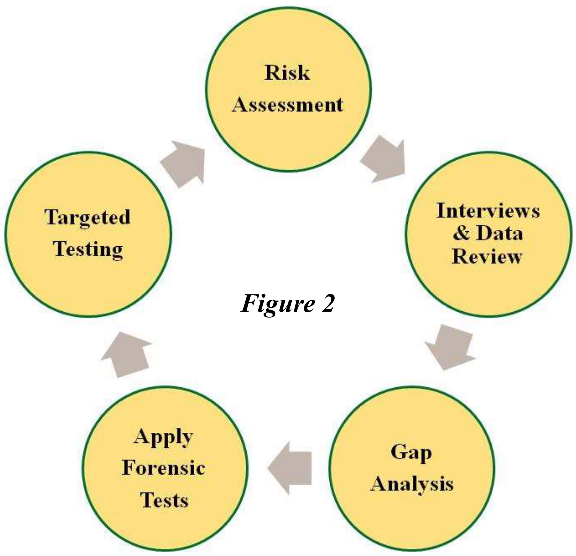


Figure 2

- fall outside an expected "norm" based upon historical patterns,
- possess high-risk characteristics typically associated with fraudulent activity,
- appear to be in contravention of company policy,
- are being accounted for in a manner that is potentially violative of the Books and Records provision of the FCPA,
- have higher rates of occurrence in one or more locations when benchmarked across the company or a discrete region, and
- Appear to be consummated at less than fair value or for no value at all.

Applying these analytical procedures is not limited to behaviors and transactions focused solely on anti-corruption matters, but can be successfully employed to detect embezzlements, kickbacks, accounting irregularities, and a host of other compliance failures and operational risks.

IV. Addressing Risks from Third Parties

Third parties continue to be a primary source of anti-corruption exposure for companies. To mitigate third party risk, companies should employ a two-pronged approach. As illustrated below, companies can look to mitigate risk during the onboarding phase[1] as well as during the post-onboarding phase. The balance of this section will discuss the post-onboarding phase.

Mitigating Third Party Risk → Pre-Onboarding Diligence

Mitigating Third Party Risk → Data Analytics/Monitoring

Most problematic business dealings with third parties are at their essence a form of embezzlement – the funds required to pay bribes are being funneled out of the company in an irregular, non-economic exchange transaction. As a result, when designing a data analytics plan, it is important to consider that violations of company policy and various statutes can be accomplished by manipulating procurement, payroll, expense reimbursements, purchasing cards, expense classifications and journal entries.

The discussion that follows provides a brief overview of some target areas for review, and a few examples of the types of forensic procedures to employ when testing both the propriety of a transaction and its compliance with applicable Books & Records provisions.

o PROCUREMENT

The "procure-to-pay" cycle continues to be an area where fraud, waste and abuse regularly occur. Data testing should look to uncover potential anomalies including identifying transactions with third parties that may be consummated at less than fair value or for no value at all. These tests may include:

- ***Supplier Validation:*** Evaluating supplier transactions with missing, incomplete, or unexpected information reflected in the vendor master file, or not listed within the vendor master file, as well as payments made to vendors with name variations or other anomalies in their identifying information.

- ***Detailed Transaction Testing:*** Payments to third parties in high-risk categories that fail to comply with one or more policies, or appear to circumvent controls, need to be examined. This can be accomplished by identifying payments with characteristics that fall outside of company "norms" and expected attributes when compared to the total population of transactions consummated by the company.

[1] Companies have a range of offerings in the marketplace from entities that provide third-party due diligence during the onboarding phase. As such, no discussion of this service will be considered in this paper.

- **Human Resources and Payroll**

The payroll function provides individuals with the opportunity to funnel funds outside of the company for use in prohibited activities, including the payment of bribes. Analytical tests to apply might include:

- ***Employee Validation/Ghost Employees:*** Employees with incomplete data or missing key information
- ***Duplicate Employees:*** Employees with multiple addresses, telephone numbers, bank accounts and/or SSNs
- ***High Risk Transactions:*** Advances or loans that are later written-off or employees with missing deductions

- **Employee Expenses**

The ability to perform analytical testing on employee expenses is dependent in part on the robustness of the company's system for capturing employee expenses and the amount of detail provided in the electronic record. The principal focus in this area may include identifying reimbursements:

- That are made to bypass the procure-to-pay control environment,
- That fail key word tests typically surrounding anti-corruption violations, and
- For cash advances to pay for travel, entertainment, and other high-risk expenditures.

- **Petty Cash**

Analytical testing of petty cash should be performed on a case-by-case basis and is primarily dependent on the particular location's and/or geography's propensity to use petty cash. The principal focus is on whether petty cash transactions are being used to bypass the procure-to-pay and expense reimbursement controls.

- **General Ledger/Journal Entries**

While journal entries are typically not a primary area of focus in an anti-corruption investigation, depending on client feedback and other pertinent discussions with the company's Compliance professionals, some testing may be performed on:

- Entries posted outside normal business hours,
- Re-classification of expenses to the balance sheet, and
- Entries that write-off receivables.

Lastly, it is important to consider that any negative result coming from one of the tests discussed above does not constitute proof of the existence of prohibited behaviors or fraudulent transactions. In addition, careful consideration must be given to qualitative issues with the company's data and how these issues might impact the results of the tests being applied.

V. Monitoring vs. Traditional Audit Approach

Based upon findings published by the *Association of Certified Fraud Examiners*, the average fraud scheme goes undetected for roughly 18 months. With the significant exposure associated with anti-corruption violations, companies cannot afford to wait 18 months before they identify prohibited behaviors. In 18 months, the number of Books & Records violations can proliferate, potential fines and penalties can escalate quickly, and a substantial amount of funds can be funneled out of the company in the form of fraudulent transactions.

As further outlined in ***Table 1*** below, when comparing the two approaches, monitoring is a far superior protocol for the early identification and mitigation of suspect behaviors. The differences between the two approaches include the following:

Monitoring	***Traditional Approach***
➢ Evaluates 100 percent of the transactions or associated target functions	➢ Evaluates only a small percentage of transactions or targeted functions
➢ Transactions or functions requiring further review are identified in a timely fashion	➢ Transactions or functions requiring further review are identified during scheduled reviews
➢ Process is highly automated and can be repeated on as frequent a basis as required	➢ Process is somewhat predictable and is repeated periodically
➢ Automatically brings in relevant outside data (i.e., PEP lists)	➢ Outside data is considered only if it is specifically sought
➢ Leads to optimal allocation of limited internal resources	➢ Internal resources are dispatched in less than optimal fashion
➢ Timely correction of errors and identification of prohibited behaviors	➢ Errors and prohibited behaviors are not identified on a timely basis

Table 1

It is clear that the longer fraudulent behaviors are allowed to continue undetected, the degree of regulatory liabilities companies accumulate will balloon along with the outflow of critical cash flows.

VI. Program Implementation and Exception Management

A monitoring system produces the most significant benefits in organizations that approach the process in a structured manner. There needs to be a:

- Clear vision of the program's goals. Is the organization solely looking to test for compliance with company policy, or is there a broader ambition of improving management oversight by detecting and eliminating accounting irregularities, as well as potentially fraudulent behaviors and transactions? These goals will dictate the types of analytical tests performed.

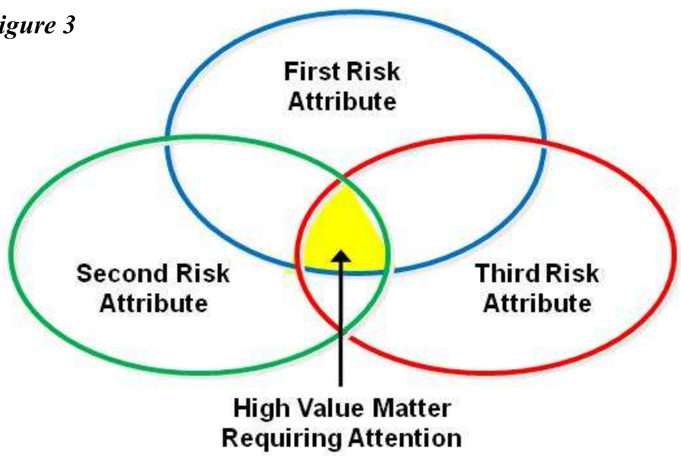
- Consensus on which data sources will be monitored, including the Enterprise Resource Planning (ERP) system, payroll and employee expense systems and system logs.

- Work-flow process in place covering the full range of actions and responsibilities, including the assignment and management of exceptions. In the absence of timely follow-up, the benefits of a monitoring system will be substantially diluted.

Lastly, there must be experienced forensic professionals involved in both designing the front-end analytical tests that drive the output, and monitoring the output generated to separate instances of real concern from the range of false positives that are inherent in this type of early warning system.

Once the monitoring system is generating exceptions, a process of managing and risk ranking the exceptions on an enterprise-wide basis needs to be in place. Without the ability to triage results, the team responsible for following up on perceived high-risk matters will find itself focusing its time on false positives and other issues that are without merit, leading to a waste of time and valuable resources. One method for prioritizing exceptions requiring further analysis is depicted in ***Figure 3***. Utilizing this approach, those transactions that fail the greatest number of analytics (and therefore possess the highest number of discrete risk attributes) represent those that rate the highest priority for follow-up and should be among the first to be assigned to a compliance and/or investigative professional for in-depth follow-up analysis and resolution.

Figure 3



VII. Concluding Thoughts

The foundation of a productive risk management solution begins with a solid system of internal controls and policies that are responsive to identified risks. Section 14(b)(2)(B) of the Securities Exchange Act of 1934 states that a system of internal controls should be sufficient to provide reasonable assurances that:

- transactions are executed in accordance with management's authorization,
- transactions and assets are recorded as necessary to permit the preparation of financial statements and maintain accountability for assets,
- access to assets is permitted subject to management's authorization, and
- recorded assets are compared to existing assets at suitable intervals and appropriate actions are taken with respect to any differences noted.

In addition to achieving the broad goals of an effective control environment, monitoring is a cost-effective solution that companies should employ as they continually test and refine their processes associated with devising, implementing, and testing their system of internal controls. Other value-added benefits include:

- Early detection of behaviors and transactions that violate anti-corruption statutes translates into reduced losses as well as significant reductions in both the number of Books and Records violations, and the amount of potential disgorgement of tainted gross profits.

- Finite internal resources are focused on operations that pose a heightened risk of theft of assets by insiders, accounting irregularities and exposure stemming from corruption risk. This allows the internal watch-dog functions to operate effectively with reduced headcounts.
- Timely detection of control weakness and non-compliance with policies provides the company with the option of implementing the required remediation on a schedule set internally rather than at the behest of regulators.
- Newly enhanced controls instituted to mitigate identified control weaknesses stemming from previously conducted analyses can be monitored to determine their effectiveness.
- Compliance with the Books and Records provision of the FCPA can be evaluated on a periodic basis allowing the Company to take timely, remedial actions when necessary.
- Recent acquisitions can be monitored to determine their level of compliance with policies and controls instituted by the acquiring company that are intended to minimize fraud risks and exposure resulting from non-compliance.
- Management can identify areas of inefficiencies and waste, as well personnel that would benefit from additional training.
- Findings of policy violations, high-risk transactions and control weakness by location can be benchmarked across the company or a particular region to determine patterns requiring additional scrutiny.
- The qualitative nature of the data being captured by location can be analyzed and augmented to ensure that the data necessary to monitor conditions and perform necessary forensic tests is being effectively captured.

Clearly, the costs associated with delayed detection, and in some cases a complete lack of detection, are substantial. In addition, the observed trends in the sphere of forensic investigations are quite troubling. There is a growing sophistication and aggressiveness of the schemes being perpetrated, a rise in the prevalence of conspiratorial relationships inside companies, and a mounting awareness among those perpetrating frauds of the investigatory protocols being employed by forensic experts. Each of these conditions poses unique challenges that require thoughtful and reasoned responses that must continue to evolve. The unfortunate truth is that you cannot stop fraud from occurring; however, you can implement solutions to detect prohibited behaviors and fraudulent transactions quickly, shut them down in their infancy, and implement additional controls to further enhance existing systems.

About the Author

Mr. Harfenist has over 30 years of investigative experience, having directed investigative teams on some of the most high-profile investigations in U.S. history, including the Tyco, Enron, and AIG matters. He possesses extensive, hands-on expertise leading multi-disciplinary forensic teams in government-initiated investigations, including matters implicating the FCPA, matters where allegations of asset misappropriation by insiders and financial statement manipulations are present.

He is an expert in the application of forensic tools used to identify anomalous transactions and high-risk relationships. His engagements have spanned the globe and have at times required the deployment of multiple forensic and document review teams in excess of 100 individuals lasting up to 3 years. He is a CPA and earned his MBA from the Jones School of Management at Rice University, where he was one of the top 5 graduates in his class. Mr. Harfenist can be reached at 713-417-9150 for any follow-up questions.