

AN OFFERING FROM THE BDO GOVERNANCE AND FINANCIAL REPORTING CENTER

CONTINUOUS MONITORING

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

A BRIEFING FOR BOARD MEMBERS, GENERAL COUNSEL,
COMPLIANCE PROFESSIONALS AND OUTSIDE COUNSEL



The responsibilities of corporate governance and risk management are becoming increasingly inseparable, with the former being the rule maker and the latter, the protector. Oversight of risks stemming from exposure to corruption and fraud is top-of-mind for executives and their advisors – and with good reason. Today's heightened regulatory environment is producing an unprecedented growth in the value of fines and the wide spectrum of costs associated with reputational damage. These risks are further exacerbated by the double edged sword of increasing compliance obligations in the face of limited internal resources being stretched to the breaking point. So what are a company's options when it comes to implementing and monitoring an effective and integrated suite of compliance programs designed to mitigate risk?

One approach, as explored in this paper, is to identify the appropriate information/data and recognize how to design and implement the proper analytics to aid management and boards in their decision-making. Organizations generate and maintain tremendous amounts of data. The power to harness such data and apply analytical tools and procedures to identify problematic trends, uncover high risk relationships and identify non-economic transactions using entire data populations in real-time can significantly impact both operational and risk management decision-

BDO USA CORPORATE GOVERNANCE PRACTICE

BDO USA's Corporate Governance Practice was developed to provide guidance to corporate boards. The firm works with a wide variety of clients, ranging from entrepreneurial businesses to multinational Fortune 500 corporations, on a myriad of accounting, tax, risk management and forensic investigation issues.

CONTACT

JEFF HARFENIST
713-576-3401
jharfenist@bdo.com
[Bio](#)

making, and can lead to the early identification and termination of fraud schemes.

The remainder of this paper outlines a suggested protocol for applying data analytics 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.

I. WHAT IS CONTINUOUS MONITORING?

Continuous Monitoring involves the integration of sound forensic practices with technology based tools to detect high risk behaviors and transactions, as well as evaluate policy compliance within an organization's financial and operational environment. Continuous Monitoring systems can identify, quantify and report in real time instances of non-compliance with company policy, high-risk behaviors and transactions, as well as failures in the internal controls. Unlike traditional sampling techniques that result in analyzing only a fraction of the available records in a data set, Continuous Monitoring examines 100 percent of the population of records, leading to much greater coverage and reduced risk.

Continuous Monitoring systems can also identify high-risk operations within a company's global business by testing for suspicious trends, data inconsistencies, duplications, policy violations, missing data, and a host of other high risk attributes. These tests can be performed remotely, and based upon the reported results, the appropriate compliance and forensic experts can be routed to those geographic areas posing the greatest risk of loss and exposure. This produces increased efficiency, reduces travel costs and allows companies to focus finite resources on their highest and best use.

II. CONDITIONS DRIVING THE NEED FOR CONTINUOUS MONITORING

Devising, implementing and testing a system of sound internal controls are all critical to the process of promoting and monitoring sound financial management practices, mitigating the risk of fraud, and defending against derivative suits alleging a defendant's failure to establish and maintain sufficient anti-corruption compliance controls. A review of the interrelated forces converging within the corporate sector is vital to understanding the mounting risks associated with fraudulent behaviors. Combating these forces requires the implementation of innovative applications to mitigate an organization's overall fraud and corruption risk. The range of forces includes:

- ▶ **Global Corporate Focus:** Significant profit opportunities abound within emerging markets in South America, Asia, the Middle East and Africa. However, these economies pose extremely high fraud and corruption risks due to the existing business and cultural practices which often run afoul of western anti-corruption statutes and operating norms.
- ▶ **Emerging International Anti-Corruption Standards:** Many countries, including Canada, Germany, China – have recently announced measures to strengthen their anti-corruption statutes and expand the associated fines for offenders (Russia's Federal Anti-Corruption Law No 273 effective 1/1/13 and the Brazilian Clean Companies Act effective 1/29/14). These measures, which are in addition to the UK Bribery Act (effective as of July 1, 2011) and the long-standing Foreign Corrupt Practices Act, will increase the corruption related risks for companies conducting business in these markets.
- ▶ **Continued Focus of US Regulators:** The DOJ and SEC continue to initiate enforcement actions and prosecute corporate insiders involved in alleged bribery schemes. In 2013 and 2014 the SEC initiated 17 actions while the DOJ initiated 26.
- ▶ **Penalties Assessed:** Over the past 10 years there has been a steady uptick in the cost of resolving enforcement actions with the SEC and DOJ. For 2013 and 2014 the average total value of FCPA enforcement actions approximated \$80 million and \$156 million, respectively. It is clear that the cost of non-compliance with anti-corruption statutes continues to pose significant financial risk.
- ▶ **Dodd-Frank's Whistleblower Provision:** The Dodd-Frank Act of 2010 provides whistleblowers a 10 to 30 percent bounty of recoveries in excess of \$1 million. Given the substantial average settlement with US regulatory bodies over the last two years and the associated reward this would produce, the likelihood that an employee uncovering behavior that violates anti-corruption statutes will go directly to the US Government and bypass a company's internal reporting channels increases exponentially.
- ▶ **Shareholder Derivative Suits:** Entities that disclose instances of suspected or actual violations of anti-corruption statutes may find themselves embroiled in costly class action civil litigation. A number of companies, including *Key Energy, Alcoa, and Cobalt International Energy* defended allegations including breaches of fiduciary duty and claims that they failed to establish and maintain sufficient anti-corruption compliance controls.
- ▶ **Length of Time to Detection:** According to the *2014 Report to the Nations on Occupational Fraud and Abuse* published by the Association of Certified Fraud Examiners, the average fraud scheme continues undetected for approximately 18 months. Based upon this finding, not only will the losses flowing out of a company compound over such an extended period of time, but from an anti-corruption perspective, a company's Books and Records and disgorgement exposure will escalate substantially as infractions mount and tainted sales occur.
- ▶ **Finite Resources:** Budgets for compliance professionals and internal auditors are continually under pressure as companies seek to improve reported results by streamlining operations and reducing non-revenue generating expenditures. However, placing constraints upon the internal watch-dog function at a time of escalating risk only serves to increase the likelihood of prohibited behaviors, violations of applicable laws, non-economic transactions, contravention of company policies, and questionable relationships going undetected.

When the operational pressures associated with each of these factors are considered in their totality, there is a clear need for a technology driven approach that mitigates the risks stemming from these conditions in a cost effective and efficient manner. Continuous Monitoring is a responsive solution.

III. CONTINUOUS MONITORING PROVIDES A RISK MITIGATION SOLUTION



Figure 1

Conducting forensic investigations into potentially fraudulent practices can be labor intensive and inefficient in the absence of a properly focused engagement team, and the thoughtful application of forensic tools by qualified experts. As a result of the complex interrelationships that exist between a company's operations and its control environment, the investigative process needs to be iterative. The systematic approach depicted in **Figure 1** 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 of an operating entity located abroad. With limited exception (i.e., conducting in-person interviews), each of the analytical procedures highlighted in Figure 1 could be conducted, in whole or in part, using Continuous Monitoring. For example, consider the process of performing an entity-level risk assessment across a global organization in order to optimally focus finite company resources. Putting aside the more elementary anti-corruption risk factors, such as conducting operations in countries with a known culture of corruption, and the use of agents and other third party intermediaries, a Continuous Monitoring solution can identify the frequency of a number of other attributes possessing high indicia of fraud. These would include transactions that:

- ▶ 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 in violation of the Books and Records provision of the FCPA;

- ▶ Have a higher rate 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, kick-backs, accounting irregularities, and a host of other compliance failures and operational risks.

IV. CONTINUOUS MONITORING VS. TRADITIONAL INTERNAL AUDIT APPROACH

As mentioned previously, the average fraud scheme goes undetected for approximately 18 months. When compared to the traditional intermittent, sampling-based approach utilized by most internal audit departments, this is not at all surprising. With the continually increasing risks associated with anti-corruption exposure, companies cannot afford to wait 18 months before their systems identify potentially anomalous transactions and high-risk relationships. Within this period of time, the number of Books & Records violations can multiply significantly, and substantial amounts of funds can be funneled out of the company in non-economic transactions.

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

Continuous 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 real-time	▶ 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 automated and is repeated on periodically as determined by Internal Audit
▶ Automatically brings in relevant outside data (i.e., PEP ¹ 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

1 PEP – Politically exposed person (PEP) is a term describing an individual entrusted with a prominent public function, or a relative or known associate of that person. A PEP generally presents a higher risk for potential involvement in bribery and corruption based on the nature of their position and potential influence.

It is clear that the longer fraudulent behaviors are allowed to continue undetected, the degree of liabilities companies accumulate will balloon along with the outflow of critical cash flows. In the following section, we will explore the application of Continuous Monitoring.

V. APPLYING FORENSIC DATA ANALYTICS TO ANTI-CORRUPTION

The detection of prohibited payments, dubious relationships and high risk activities represents a few of the central elements in both proactive and reactive anti-corruption engagements. When designing a forensic data analytics plan, it is important to consider that violations of company policy and/or various statutes can be effected by manipulating accounts payable, accounts receivable, payroll, expense reimbursements, purchasing cards, expense classifications and journal entries. The balance of this section provides a brief discussion of some target areas for review, and a few examples of the numerous forensic procedures that can be deployed to test both the propriety of a transaction and its compliance with applicable Books & Records provisions.

ACCOUNTS PAYABLE

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:** Suppliers with missing, incomplete or unexpected information reflected in the vendor master file or not listed with the vendor master file.
- ▶ **Duplicate Suppliers:** Payments made to vendors with name variations or other anomalies in their identifying information.
- ▶ **Unexpected Relationships:** Common identifying characteristics across the spectrum of the employee/vendor/customer relationships.
- ▶ **Detailed Transaction Testing:** Supplier payments without invoices, payments to/invoices from excluded suppliers, and payments with characteristics that fall outside of company “norms” and expected attributes.

ACCOUNTS RECEIVABLE

Manipulative activity in accounts receivable provides a conduit for employees seeking to direct value to government officials in forms other than direct cash payments. The data tests are comparable to those described above with the difference being the focus on customer relationships, and may include:

- ▶ **Customer Validation:** Customers with unusual addresses, missing physical address elements or unexpected information in their customer profile.

- ▶ **Duplicate Customer:** Customers with name variations or other anomalies in their identifying information.
- ▶ **Unexpected Relationships:** Common identifying characteristics across the spectrum of the employee/vendor/customer relationships.
- ▶ **Detailed Transaction Testing:** Consists of a number of tests including sales to customers with unexpected rebates, excessive credit memos or other unusual characteristics that fall outside of company “norms”.

HUMAN RESOURCE 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/Fictitious Employees:** Employees with incomplete data or missing key information.
- ▶ **Duplicate Employees:** Employees with multiple addresses, telephone numbers, bank accounts and/or SSNs.
- ▶ **Unexpected Relationships:** Common identifying characteristics across the spectrum of the employee/vendor/customer relationships.
- ▶ **High Risk Transactions:** Advances or loans that are later written-off or employees with missing deductions.
- ▶ **Unauthorized Transactions:** Employees receiving inflated overtime hours and payments, or other forms of compensation post separation.

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 analytical focus in this area may include identifying reimbursements:

- ▶ Made to bypass the procure-to-pay control environment,
- ▶ That fail key word tests typically surrounding anti-corruption violations,
- ▶ For cash advances to pay for travel, entertainment and other high risk expenditures, and
- ▶ That continually approach authority levels.

PETTY CASH

Analytical testing of petty cash is done on a case by case basis and is primarily dependent on the particular location’s and/or geography’s propensity to use petty cash (i.e., China). 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 Internal Audit and Compliance professionals, some testing may be performed on:

- ▶ Entries posted outside normal business hours,
- ▶ Re-classification of expenses to capital assets, 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.

VI. CASE STUDY

To illustrate the benefits of a Continuous Monitoring program, a case study based upon an actual investigation is presented below².

ASSUMED FACTS

- ▶ A NYSE listed company has a subsidiary in South America that provides high-end engineering and project management services for large-scale infrastructure projects.
- ▶ To mitigate the risk of fraud and corruption, sub-contractors and/or vendors seeking to work on Company projects need to submit to a rigorous approval process.
- ▶ Once approval is granted, invoices and/or draw requests will be processed by the Company, and paid within 50 days pursuant to its standard accounts payable policy.
- ▶ A payable cannot be established to a sub-contractor or vendor who is not in the vendor master file, and as a result, no payments can be made to unauthorized entities.
- ▶ Tight controls exist over access to the vendor master file.

An internal investigation conducted towards one project's completion determined that Company insiders had funneled in excess of \$1 million out of the project over a 34 month period using multiple schemes. Additionally, the investigation revealed that by virtue of the positions the perpetrators held in the Accounting and Procurement functions, they clearly understood:

- ▶ The control environment and how collusive behavior could bypass existing controls;

- ▶ Nuances within the cost accounting system that could be exploited to their advantage, and
- ▶ How project variances would be identified and evaluated by those tasked with reviewing the project's metrics against budgets.

As a result, the insiders were able to subvert internal controls, bypass the internal monitoring functions, and exploit their understanding of project variances to insert scores of bogus invoices into the system and receive a continuing stream of payments. The following section will discuss the schemes - and their detection - in greater detail.

DETECTING THE FRAUD

This section addresses two of the primary schemes employed by the perpetrators to funnel money out of the company for unauthorized use, and how the analytics employed by a continuous monitoring system would have detected these schemes and shut them down in their initial stages.

- ▶ **Scheme #1:** At the outset of the project, numerous vendors submitted proposals to provide security services to protect machinery/equipment, inventory, supplies, and personnel. During the due diligence phase, it was determined that one such company seeking approval - **Vendor A** - was partially owned by a government official, and as a result, was not selected. However, shortly after the project commenced, monthly invoices were submitted by **Vendor A** and were subsequently paid. Each payment was recorded in the company's general ledger under the expense classification "Security Services". The payments were made via wire transfer.

Services present a unique forensic challenge when it comes to analyzing them after the fact, as unlike the purchase of hard assets, you are often unable to verify their delivery. However, in this instance, the analysis revealed that the outgoing wires to pay **Vendor A** had not been cleared through the Accounts Payable system, but were directly impacting an expense account - a clear indication that company policy was being circumvented. A continuous monitoring program tracking policy compliance would have identified this scheme very early on, saving the company substantial amounts of money and preventing in excess of 30 Books and Records violations.

- ▶ **Scheme #2:** Due to the magnitude of the project, internal headcounts were insufficient to staff various technical aspects of the project. As a result, a portion of the technical work was performed by sub-contractors, a common practice that would not have raised suspicion. However, a little over twelve months into the project, **Vendor B** was added to provide additional sub-contractors to the existing pool of vendors that had been approved at the project's outset. The problem is that **Vendor B** was a sham which provided no discernable benefits to the project.

² Significant facts, such as the location of operations and business types have been altered to protect client confidentiality.

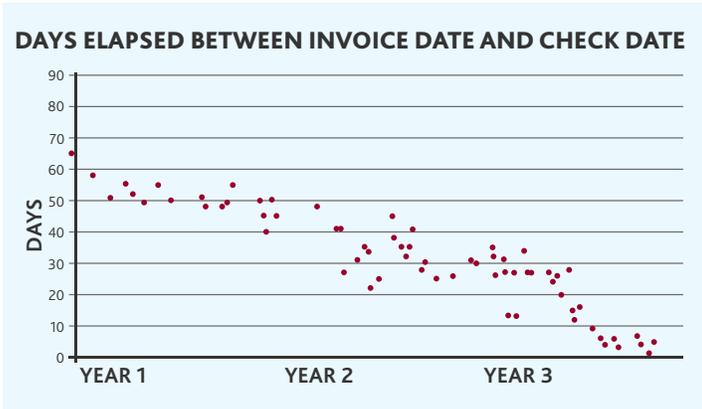


Figure 2

Figure 2 presents the results of a forensic test that compared the elapsed time between the date of an invoice and the payment associated with that invoice for a specific sub-classification of vendor expense data. Several conclusions are evident from the data presented in Figure 2. First, a regression plotted through this data will generate a downward sloping trend line that approaches zero. This attribute is highly suspicious and would warrant further analysis.

Second, and more importantly, by segregating the data presented in Figure 2 into two subsets with similar attributes, you arrive at what is depicted in Figure 3 below. The first box outlined in red on the left side covers all of the recorded transactions in Year 1, each of which occurred prior to the addition of Vendor B. This data presents a pattern that one would expect to observe based upon the expected frequency and payment policies for the particular services rendered. However, beginning in Year 2 and continuing into Year 3, the data outlined in the 2nd red box on the right side of Figure 3, displays data with both a different frequency profile and a steadily declining gap between payment dates and invoice dates. Both of these payment attributes are problematic when considered on their own. However, when occurring together you have a clear sign of serious problems warranting immediate investigation. A continuous monitoring program analyzing transactional relationships would have identified these anomalies early on in Year 2, saving the organization more than \$1 million in losses, as well avoiding the occurrence of approximately 40 Books and Records violations.

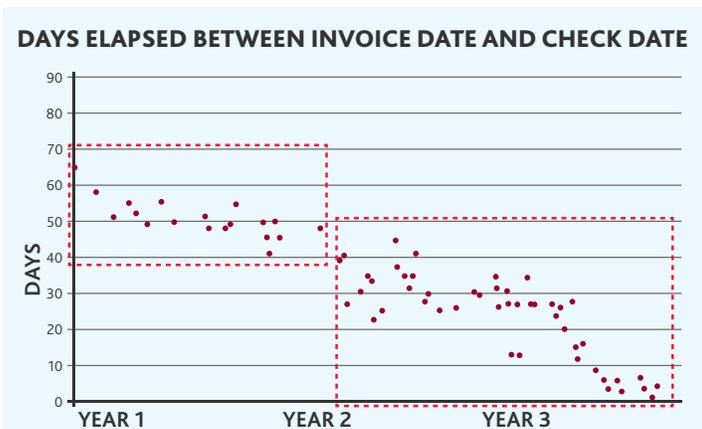


Figure 3

While the investigative procedures discussed above are illustrative of the broad spectrum of tests available to forensic professionals, the total pool of analytical tests is as varied as the nature of issues one is looking to uncover.

PROGRAM IMPLEMENTATION AND EXCEPTION MANAGEMENT

A continuous monitoring system produces the most significant benefits in organizations that approach the process in a structured manner. First, there has 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 decisions will dictate the types of analytical tests to perform. Second, there must be consensus on which data sources will be monitored, including the Enterprise Resource Planning (ERP) system, legacy systems and system logs. Third, it requires a keen insight into the underlying data that will be mined - which is not always as clear as it may seem. For example, do the recorded cash disbursements represent transactions initiated through the ERP system, or are they being recorded post issuance - producing underlying data that may lack integrity. Fourth, there needs to be a 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 continuous 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 system, and monitoring the output generated in order to separate instances of real concern from the range of false positives that are inherent in this type of early warning system.

Once the continuous 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 effectively triage results, the team responsible for following up on perceived high risk matters will find itself focusing its time on an abundant number of 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 review and analysis is depicted in Figure 4. Utilizing this approach, transactions that fail the greatest number of analytics (and therefore possess the highest number of discrete risk attributes) represent those that rate the utmost priority for follow-up and should be the first to be assigned to a compliance and/or investigative professional for in-depth analysis and resolution.

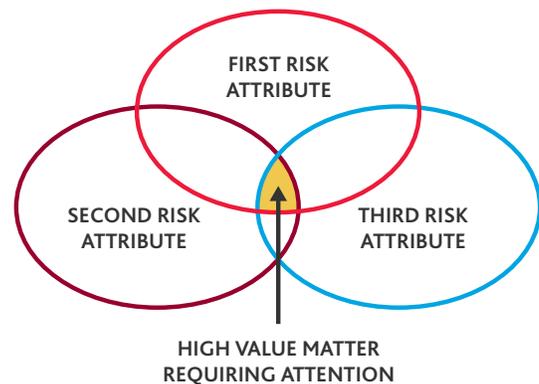


Figure 4

VII. CONCLUDING THOUGHTS

The foundation of any meaningful risk management practices begins with a solid system of internal controls. Section 13(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 (1) transactions are executed in accordance with management's authorization; (2) transactions and assets are recorded as necessary to permit the preparation of financial statements and maintain accountability for assets; (3) access to assets is permitted subject to management's authorization; and (4) 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 that are discussed above, continuous monitoring is a cost effective solution that companies should consider incorporating as they continually 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 across company 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 without expanding 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 timely 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 the level of compliance with policies and controls instituted by the acquiring company in order to minimize fraud risks and exposure resulting from non-compliance;
- ▶ Findings of policy violations, high risk transactions and control weakness by location can be benchmarked across the company or a particular region, and
- ▶ The qualitative nature of the data being captured by location can be analyzed and augmented to insure 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 high and are escalating at an ever increasing rate. 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.

For more on data analytics and mitigating risks, refer to BDO's archived webinar and self-study course: [2015 Board Matters – Data Analytics and Risk Management: A Board Primer](#).

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, financial advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through 63 offices and more than 450 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,328 offices in 152 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

© 2015 BDO USA, LLP. All rights reserved.