Data analytics is a powerful tool to prevent fraud and manage risk

Identify risk of noncompliance with anti-corruption laws

Data analytics should be a key weapon in every company’s fraud protection arsenal. The truth of every company’s operations is in the data. By using data analytics, companies can use that data to identify indications of fraud and to develop proactive steps to minimize the risk of future fraudulent acts.

Addressing fraud and remaining in compliance with local and international anti-corruption laws has never been more important. Companies are under increasing pressure to effectively and transparently improve their corporate governance practices. Large-scale financial scandals and increasing scrutiny of corporate behavior by the general public are factors pushing companies to ramp up their efforts to control fraud. In addition, international government regulations, such as the U.K. Bribery Act, The People’s Republic of China anti-corruption laws, the Brazilian Clean Companies Act and the Foreign Corrupt Practices Act (FCPA), require compliance with applicable local and international anti-corruption laws, furthering the need for fraud and risk management.
Identifying, controlling and ultimately deterring fraud can be challenging for a number of reasons:

- No business process or control is perfect. You need effective testing and enforcement mechanisms to support your control environment.
- Compliance resources must be allocated effectively. Across every area of operations, companies must do more with less to compete today. Your control environment is no exception. Data analytics can help you leverage your technology infrastructure to identify and protect against fraud more quickly and efficiently.
- Pressure to perform can motivate employees to behave inappropriately to meet certain metrics. Not every fraud starts with an employee looking to steal from the company. The unintended consequence of some performance measurement strategies can be a motivation for employees to try to game the system through inappropriate actions.
- Collusion is difficult to identify and harder still to prove. When someone within your organization decides to cooperate in a fraud with another party, it can be difficult to isolate and identify that behavior — especially if the party involved has some knowledge of your control environment. Data analytics can help.
- No matter how effective your controls or how strong your corporate culture, there can always be an employee bent on fraud.

Data analytics versus audit-based approaches

So how does data analytics help? Traditional internal controls rely on an audit-driven approach. Whether conducting typical internal audit procedures, or in response to a suspicion of fraud, auditors often rely on a statistical sampling methodology. Because this, by definition, means they do not look at all data, they tend to focus on the largest transactions, or those with the highest perceived risk. That approach means that vast amounts of data are rarely considered. Fraudsters smart enough to conduct their improper activities in smaller steps, and in ways that do not appear inherently risky, could avoid detection for years and misappropriate huge sums as a result.

In contrast to traditional methods, data analytics generally does not rely on sampling of documents. Rather, in most cases, the use of effective forensic data analytics techniques provides the ability to analyze the entirety of the population of the electronic data available for a given scenario, and to look for connections or other unusual characteristics that might indicate fraud, enabling you to then target high-risk transactions for further examination.

Certain types of transactions have inherently higher levels of risks and are candidates for closer analysis. These include:

- Payments to risky vendors, including reimbursement expenses to business development personnel who deal with government officials nationally or internationally
- Payments made from and to foreign bank accounts
- Use of new attorneys, accountants, consultants or other professionals with no prior relationship to the company, including payments out of the norm relative to historical patterns to such entities
- Suspicious payment transactions, such as for services rendered missing proper support, donations, lavish entertainment expenses, gifts, facilitation expenditures, trips with undocumented or unclear business purpose, etc.
- Payments made to entertain government-related personnel
- Transactions that vary widely from norms — that could mean a transaction for an amount that falls outside the usual amount in a category or for a vendor
- Journal entries with non–typical or infrequent large offsets to cash account credits — this may indicate someone plugging a less scrutinized ledger account to force cash reconciliations with the objective to conceal an embezzlement scheme
- Top-slice journal entries increasing income, especially where additional unusual characteristics are noted, such as the time of booking, rounded dollar amounts that may indicate estimates, etc.
- Manual adjusting entries recorded at the corporate level, often when preparing consolidated financial statements for subsidiaries. Although such entries can be valid, they can be used to perpetuate fraud by improperly presenting a more favorable picture of the actual operating results reported to the investing public and other entities that rely on the company’s financial statements. The incentive is a personal gain via a bonus, raise, promotion, or even just continued employment where concerns of performance have been in question

Data analytics can also support your due diligence during a merger or acquisition. After all, you aren’t just acquiring a company, you are also acquiring its liabilities, including the consequences for any fraudulent or other inappropriate acts. And, as with every other area of your business, taxes matter. There can be serious penalties and tax consequences for misrepresenting questionable payments in your books and records.
How data analytics works

The easiest way to illustrate the power of data analytics is by example. Consider the issue of collusion. This can be very difficult to detect and prove. Suppose an employee within the company decides to collaborate with someone at a vendor in a kickback scheme. The employee knows that amounts paid in the scheme should be kept below a certain threshold to avoid the need for approval from higher levels and attention from internal audit. The vendor is already set up in your system as an approved payee. So the employee arranges for a second account with the vendor and has regular payments to that account sent to a separate address so that they are not detected by the vendor’s controls. Then, the collaborating party at the vendor collects those payments. This is the kind of scheme that traditional internal control efforts often miss.

Through data analytics, however, indications of such a fraud can be discovered. The transactions and other data extracted from the source systems can be analyzed to flag accounts with more than one address for payments. Also, in schemes where employees create an additional vendor account, that account is then usually used only for those fraudulent payments, so questionable payments in some instances are linked to invoices with unusual characteristics including but not limited to consecutive invoice numbers, changes to the patterns in the structure of invoice numbering nomenclature and substantial variations from the historical amounts of invoices paid to that vendor. A trained forensic investigator using data analytics can segregate and rank invoices and payments with unusual characteristics by risk level for subsequent inspection.

Does that mean that every account with multiple addresses that is paid consistently with the same amount or that presents other unusual characteristics is fraudulent? Of course not. You may have started doing business with an existing vendor, but in a different location, or you may have entered into a consulting agreement that calls for quarterly payments of a set amount. The point is that your data can be forensically reviewed to flag patterns that are more frequently associated with fraud, thus surfacing them for further examination. Some of that examination can also be automated and reported near real time. For example, through joint data element testing, the address and telephone information for a suspicious vendor account can be compared with the same information for your employees. If matching data elements are found, you could automatically provide an alert to a designated officer to determine if the employee and vendor relationship is in compliance with company policy.

An even more comprehensive approach to a data analytics strategy involves the access of external public records to highlight specific characteristics in the data provided by vendors and employees. For example, vendor addresses can be compared to public databases to determine if an address is residential or commercial, if occupants at the address change frequently, or if the address is flagged as vacant, invalid, or is missing a unit number or other information. Vendor telephone numbers can be compared to public sources to determine if the telephone number is valid and to check for other discrepancies, such as a phone number listed to a P.O. Box; if it is a mobile or cellular number; or if a land line is mismatched with the vendor ZIP code. Information automatically collected from the Internet through data-harvesting techniques can be used to check for issues such as whether vendor and employee addresses or telephone numbers have been claimed by other entities with different names in the recent past.

Consider the following situation. Suppose you found all of the following issues involving an active vendor receiving substantial payments:

- The only contact number you have on file for the vendor is a mobile number
- The ZIP code of the address provided by the vendor does not exist according to the U.S. Postal Service tables
- The invoices associated with the vendor displayed unusual characteristics, such as inconsistencies in the codification of invoice numbers

Clearly, you would be concerned. These are just the sorts of issues that data analytics can uncover — and that might be missed by traditional audit-based internal control measures. Using data analytics to examine relevant public information and in the forensic analysis of your internal data can be a powerful tool to detect and deter fraud.

A powerful tool to manage off-shore risk

The enhanced fraud prevention capabilities inherent in data analytics can be particularly useful to companies in today’s increasing global business environment. Certain activities considered illegal under U.S. law, particularly under the FCPA, could be seen as customary in other regions of the world. Awareness of exposure to the FCPA and its often substantial penalties must be proactively and clearly communicated to your personnel while conducting business directly or through intermediaries in foreign markets.

U.S. laws are not your only concern. For instance, the United Kingdom’s Bribery Act of 2010 can often apply to U.S. businesses with connections to the United Kingdom, and its provisions, in some instances, are even stricter than the FCPA’s.
Part of effective compliance with FCPA and other pertinent laws is a macro-level understanding of where your risks reside. In many foreign markets, industries such as energy, health care and transportation have a high level of government participation or even ownership. Since FCPA violations often involve corruption or other inappropriate interactions with government officials, such industries carry a higher level of risk.

Compliance with FCPA and local laws can be especially challenging for middle-market firms making their first forays into a foreign market. They will often be approached by local officials or other contacts with schemes that are represented as the normal way of doing business in that market — and that may be true. But if the normal way of doing business is a violation of FCPA or another applicable law, then that activity is still illegal.

Having the right data in the first place is vital to making data analytics work — and this can be especially true in foreign markets. However, while you will want to collect the necessary information on employees, vendors and customers to make data analytics work, you also need to carefully consider the applicable privacy laws in each country.

Companies also need to understand that they can’t evade responsibility for FCPA by using intermediaries or other third-party relationships. You are likely to end up on the hook for any fraud, bribery or other inappropriate activity such parties undertake on your behalf. Data analytics can be useful as you extend the enforcement of your corporate policies to cover those parties and their activities.

FCPA compliance is a serious issue. Penalties for FCPA violations can run into the millions of dollars. You could even lose your export privileges or your ability to do business with the federal government. And the legal consequences for individuals involved can also be very dire. Data analytics can help.

**A wide range of benefits**

We’ve described a few examples of how data analytics works. Following are some of the key ways in which it can strengthen your overall corporate compliance strategy:

- It’s more efficient. The process can be highly automated and can broaden the reach of your internal control efforts beyond statistical sampling to include all data.
- It’s more effective. Because data analytics surfaces those transactions most needing attention, your people spend less time looking at transactions that are unlikely to be a problem and more time analyzing those likely to be fraudulent.
- It identifies opportunities for improvement. Data analytics can help highlight current weaknesses in your operating procedures and control environment. Obviously, it gives you the chance to evaluate the issues that made previous frauds possible. But, by also identifying suspicious activities that turn out not to be fraudulent, it can help you consider whether those procedures or controls underlying those transactions should be modified before they are exploited for fraudulent purposes.
- It not only strengthens your controls, it sends a clear message to your people. Most employees are good, hard-working people looking to build careers and help your company. But an important part of any fraud prevention program is sending a strong deterrent message to employees who might consider fraud. By making it clear that all data is now being evaluated, employees are less likely to think they can avoid detection just by gaming known control parameters.
- It can even spotlight wasteful practices. For example, those multiple vendor accounts? Maybe they weren’t opened to perpetrate fraud, maybe they were opened because you don’t have clear procedures around how to set up, document and control your activities such as the monitoring of duplicate payments with each vendor. Waste might not be a crime, but it can be equally destructive to your bottom line.

The breadth of data collected by today’s information technology systems is staggering. Companies should be leveraging that data by using data analytics to increase the effectiveness of their fraud prevention and corporate compliance efforts. A well-designed data analytics strategy can strengthen your internal controls, help you better enforce your corporate policies, proactively manage risk in an increasingly globalized economy, identify waste and improve existing business processes.