COSMOS
Navigate the Compliance Universe

CEP Magazine - December 2021
Data-driven risk management: Detect fraud before the tip-off

By Parth Chanda, Esq., and Greg Bates, JD

Parth Chanda (pchanda@lextegrity.com) is Founder and CEO of Lextegrity, based in New York City. **Greg Bates** (gbates@milchev.com) is Counsel for Miller & Chevalier in Washington, DC.

An estimated 43% of occupational fraud is detected by way of a tip—or whistleblower report—according to the latest edition of the Association of Certified Fraud Examiners' *Report to the Nations.*[1] That's a huge proportion, and one that emphasizes the value of reporting channels as a method for detecting occupational fraud schemes.

But tips often come too late. What's more, not every fraud scheme is detected internally—if at all.

This raises obvious and tantalizing questions: What if it was possible to detect occupational fraud schemes earlier, and what if it was also possible to detect those schemes at a much greater rate?

For a growing number of forward-thinking enterprises, this seemingly unreachable goal is becoming a reality. For them, the solution lies within data-driven risk management.

What is data-driven risk management?

Data-driven risk management describes the prioritization of data insights (from inside and outside your organization) to assess and manage risk holistically.

The use of data to support business strategy and decision-making is nothing new. Business functions like marketing and sales have used data insights to assess, predict, and capitalize on revenue growth opportunities for decades. However, the traditional approach to using data within a risk management context has typically been siloed, making it almost impossible to see potentially useful data within a meaningful broader context.

When it comes to detecting fraud, hotline reports have long been a key detection tool. Yet frauds detected in this way mean any related data tends to be historic (and often well after a financial crime has been committed), lacking in quantitative detail, and only available if a report is submitted at all.

Truly effective data-driven risk management makes use of data sets from multiple sources to build a more detailed picture. Layering these various data sets on top of each other provides context, enabling compliance, risk, and audit teams to make more informed, data-led decisions. It can provide analytical data on an ongoing basis to illustrate whether existing controls are working instead of simply flagging instances where they have failed. It also makes it possible to detect financial crimes at a much earlier stage or even prevent them from occurring.

How can a data-driven approach help?

To illustrate how this can work in practice, let's take the example of the fictional corporation, Acme Inc.

Acme is investing heavily in the communities in which it operates globally, with a goal of helping local stakeholders adapt better to the demands imposed by climate change. The company has implemented a targeted donations program to support the social and environmental initiatives of local nonprofit organizations.

Historically, Acme has allowed local subsidiaries to authorize such donations within their local procurement and financial systems. Over the years, some of those donations have resulted in substantiated whistleblower complaints citing waste, abuse, conflicts of interest, and potential improper influence of local government officials.

As a result, Acme has embarked on a more proactive, data-driven approach to managing such risks. This involves combining data from various sources to detect and anticipate spend risk more accurately, as follows:

1. Acme has put into place an approval and due diligence process for vetting donations before they are made. As part of that process, Acme can compare each request against historical spend data for similar local expenditures. This allows it to see if the proposed donation is an outlier in amount, frequency, or other dimensions.
2. The due diligence process also collects background information from the receiving entity via a questionnaire. It automatically validates that information against an external database to identify adverse media, sanctions, or other reputational warning signs. This screening happens during onboarding and on an ongoing basis.
3. Acme monitors all spend items (payments) in each of its jurisdictions, applying multiple layers of fraud analytics to each payment item. These analytics check that any donation payment has completed appropriate due diligence, and that it matches the amounts and payees detailed in the due diligence approval. The analytics also scour Acme's human resources data to identify any hidden conflicts of interest, whereby the charity's attributes may match an Acme employee. The analytics look for duplicate payments, expedited payments, offshore bank accounts, and various other risk attributes.
4. Finally, the financial fraud analytics target all spend categories. Payments that may have been assigned to lower risk expense categories (to sidestep Acme's internal controls around donations) are therefore still vetted with the same degree of care. All of these analytics can be configured to place additional emphasis on countries, business units, general ledger accounts, or specific counterparties where Acme may have already identified risk.

This end-to-end data-driven approach ensures that risk management takes place in near-real time. What's more, it continues throughout the life cycle of the relationship between Acme and the counterparty. This allows Acme to proactively identify risks well before any whistleblower may become involved and, ideally, prevent a bad actor from engaging in fraudulent activity altogether.

Why should a data-driven approach matter?

There are many reasons why embracing this type of data-led approach should be taken seriously by your organization.

- **It satisfies regulatory requirements.** The U.S. Department of Justice has explicitly stated that organizations must assess the effectiveness of their compliance programs in practice and use data in pursuit of that goal. That signals a warning to organizations that relegate data analysis in favor of periodic auditing, a reactive approach to compliance risk, and subjective or biased decisioning around risk.
- **Fraud and other financial crimes can be detected faster.** A data-driven approach that tracks a range of analyses can aid the early detection and remediation of fraud and other transactional spend risks. With fraud cases lasting an average of 14 months prior to detection,[2] this early warning system can offer

obvious bottom-line benefits.

- **Your teams can focus their efforts on high-value activity.** When used effectively, a data-driven approach can provide opportunities for better-targeted efforts across the risk and compliance enterprise. For example, with ongoing access to data, risk assessments and audits can be driven dynamically, freeing your team to focus on high-risk areas.
- **Your board can make better decisions.** Reliable, contextually relevant data helps us make better decisions. Putting risk data in the hands of your board enables them to better embed risk analyses into their commercial and strategic decision-making—making your job that little bit easier.
- **You can accelerate digital transformation.** Moreover, investment in a data-driven approach enables an organization to take advantage of one of those rare leapfrog moments: They can bypass inferior legacy approaches and instead adopt a modern, superior way of working that is both more efficient and more effective at preventing and detecting risk.

Implementing a data-driven approach to reduce fraud risks

Implementing a data-driven approach to fraud detection can feel daunting, but there are some key steps that will help set an organization on the right path.

Start by understanding what data you need to collect and analyze. You can begin by identifying the relevant business processes and systems and how to access them. Employee expenses from a travel and entertainment system and vendor payments from an enterprise resource management system are great places to begin, as the data is proximate to key risks such as fraud and corruption—and is often rich and highly structured.

Once you’ve accessed that data, you will need to make sense of it from a risk perspective. This often requires specialized forensic data analytics expertise. Compliance teams often rush to visualize data in order to spot outliers or look to recruit a data scientist to help make sense of the data. However, it is typically more efficient and effective to deploy a compliance analytics tool designed specifically for this purpose.

Next, take stock of your front-end risk management processes. Do they provide a unified process for your business? If not, consider connecting them to your other enterprise systems, like your vendor master process or your procure-to-pay process. Look for opportunities to provide front-end business approvers with contextual data, as this will enable them to better assess the risks of their proposed arrangements prior to entering into them.

Finally, ensure that information from your hotline, risk assessment process, and other subjective feedback on risk is incorporated into your front-end approval and due diligence risk model, as well as your back-end monitoring model.

Data keeps you ahead of fraud risk

It’s difficult to argue with the value that hotline reporting (or more generally, tips) has offered in the detection of fraud. Yet advances in data analytics and automation provide a blueprint for the future.

Tools that pull in data from different sources, risk rate individual transactions, and visualize risk insights mean it is possible to detect fraud more often, and more quickly, than ever before. No longer do compliance teams have to rely almost exclusively on the actions of vigilant corporate citizens to gain the insights they need. Instead, they can begin to leverage their organization’s data to stay ahead of fraud—which is exactly where the Department of Justice expects them to be.

Takeaways

- Data-driven risk management describes the prioritization of data insights (from inside and outside your organization) to assess and manage risk holistically.
- "Layering" data sets from various sources makes it easier to detect compliance risk at a much earlier stage—or even prevent compliance violations from occurring.
- Embracing data-driven risk management will help you implement the updated Department of Justice guidance relating to the use of data within your compliance program.
- A data-driven approach can provide opportunities for better-targeted efforts across the risk and compliance enterprise, allowing experts to focus their time more effectively.
- Begin by understanding the data you need to analyze and gain access to it. Start with data on vendor payments and employee expenses.

[1] Association of Certified Fraud Examiners, *Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse*, accessed October 5, 2021, https://www.acfe.com/report-to-the-nations/2020/.
[2] Association of Certified Fraud Examiners, *Report to the Nations.*

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login