Leverage Data Analytics to Curb Fraud Risks

FEBRUARY 2021

Eva Weiss

Partner, StoneTurn

eweiss@stoneturn.com

+1 212 430 3423

Joshua Dennis

Partner, StoneTurn

jdennis@stoneturn.com

+1 617 570 3789

Valerie Loverro

Managing Director, StoneTurn

vloverro@stoneturn.com

+1 212 430 3420

by Eva Weiss, Joshua Dennis & Valerie Loverro

Internal auditors and others involved in compliance-related diligence work have a broad mandate to provide assurance and risk-based insights to their stakeholders, often in highly complex and heavily regulated environments.

At the same time, these practitioners recognize the need to become more efficient and more effective in identifying and responding to risks, particularly as remote work becomes the norm for many. Given that would-be fraudsters continuously innovate to avoid detection, the use of data analytics to uncover fraud risks is not new. However, audit teams are at varying levels of maturity with developing and using data-driven tools. Therefore, the key question for today's auditors is: How can you best leverage data analytics to become more empowered and efficient to better prevent, detect and remediate wrongdoing?

A key benefit of data analytics is the ability to distill large and often disparate data sets down to high-risk areas of the business (e.g., vendors, employees, transactions, etc.). This not only allows for greater coverage but also helps ensure valuable company resources are put to their highest and best use, focusing on those higher-risk areas. However, in order for a data-driven audit process to be effective in detecting actual or potential fraud, it requires careful planning focused on fraud schemes and scenarios.

After all, the external auditors must incorporate brainstorming sessions to identify fraud risks in the planning stages of their audits, as mandated by

StoneTurn

Statement on Auditing Standards No. 99, and use them periodically throughout the process. Having a similar process, with a range of participants from across the organization, is a powerful element of risk mitigation processes. Incorporating data analytics as part of such a discussion can help ensure that the brainstorming process is most productive and customized for the organization's unique structure, processes and risk profiles.

Further, articulating what can go wrong, including who could override controls or commit fraud, how they would do it and conceal it, and what it would look like (red flag indicators in the data), will facilitate building effective data analytic queries to find anomalies, patterns and trends that may be indicators of wrongdoing.

The objective is not to identify every conceivable scheme and scenario, but audit teams should identify the relevant schemes and scenarios inherent in the business processes under review, as well as their likelihood and impact. This helps to prioritize and determine which are in the audit scope.

The power of data analytics is much more effective than sampling a small number of transactions. Data anomalies are detected when looking at a full population of transactions over time and can help shed light on outliers, patterns or trends that inform the team's view of risk in those transactions.

Step 1: Gather information

Leverage the organization's risk inventory, its risk and control self-assessment (if available), and a cross-functional understanding of the processes and controls to develop fraud risk considerations within each risk type.

Determining all potential data sources available, such as the general ledger, vendor/customer lists, human resources metrics, hotline data, employee training logs and external data resources—including considering relationships between the data sets that should, or should not, be present—will drive the design of the data analytics tools. Recognizing that helpful data sources may exist outside of the organization—such as external benchmarking information, third-party due diligence and business intelligence—should be part of the process. For internal data sources, the inventory should also include important factors such as applicable timeframes (e.g., did the organization previously migrate to a new accounting system or acquire a new business?), data availability (e.g., can the audit department easily export the data or connect directly to the system?) and data integrity (e.g., are there sufficient controls surrounding who can edit data or is the data inconsistent or incomplete?).

Step 2: Articulate schemes and scenarios

Conversations among the audit team and relevant stakeholders can yield the best results—two (or more) heads are better than one! The more specific the scheme and scenario, the easier it will be to identify red flag indicators, reduce false positives, and build data analytic queries to search for them.

A successful fraudster knows how to not only

perpetrate a crime, but also how to hide it, which may involve the need to circumvent or override controls. As a result, audit teams should "think like a fraudster," and that means understanding the process and flows of information from beginning to end, including controls, control gaps, monitoring and reporting.

Step 3: Identify red flag indicators

Identify unusual circumstances or anomalies that may be indicators of wrongdoing (e.g., patterns of control overrides and exceptions; unusual transaction timing, frequency, amount or approval; or lack of segregation of duties). This process can often be aided by the use of dynamic visualizations, which allows the user to quickly explore the data and actually see patterns emerge by changing various filters or other criteria.

Step 4: Develop data analytics

Once the audit team articulates the fraud schemes and scenarios and identifies red flag indicators, then targeted data analytic queries can be developed.

For example, assume an employee has a conflict of interest with a vendor and intentionally overpays invoices in return for a kickback. In this scenario, the employee might submit legitimate vendor payment requests to accounts payable forfeiting the vendor discount, even though payment will be made within the discount period.

To detect this fraud scenario, data analytics can be used to quickly and systematically identify any vendor discount discrepancies between the vendor master file and accounts payable system. If discrepancies are identified, further analysis and testing can help rule out errors or determine if other red flags are present. For example, are there discrepancies with multiple vendors associated with only one employee?

In this example, if the employee is receiving kickbacks, this would not be visible in the company's books and records.

However, data analytics can help auditors focus on high-risk issues for further analysis and inform the investigative process.

Inside the haystack

Uncovering fraud can be difficult. Effective fraud brainstorming requires more effort than simply gathering stakeholders for an hour-long discussion of how fraud might occur. It involves delving into the details, thinking like a fraudster and using in-depth knowledge of the organization's processes and systems to increase awareness of where frauds may be hiding.

As the size and complexity of data sources within a business organization continue to expand, it is increasingly important for audit teams to focus on data analytics to help uncover those "needle in a haystack" areas for further consideration. With in-person oversight of operations less practical now, fraud risk assessments and subsequent testing must consider how data analytics can play an integral role in preventing and uncovering misconduct.

This article was initially published in **Accounting Today in February 2021**

About the Authors

Eva Weiss, a Partner with StoneTurn, has more than 25 years of experience in forensic investigations and compliance controls and monitoring for both the public and private sectors.

Joshua Dennis has more than 15 years of experience working with clients and counsel on issues requiring complex data analysis, including investigations, economic damages, intellectual property, enforcement, forensic accounting, compliance monitoring, and valuation engagements.

Valerie Loverro, a Managing Director with StoneTurn, has more than 25 years of experience in forensic investigations, and compliance controls and monitoring. Working primarily with large financial services firms, she focuses on internal audit, fraud risk assessment processes, post-investigation root cause analyses, and proactive antifraud controls and programs.