5 Ways to Reduce Compliance Risk with Continuous Compliance Monitoring

Case IQ

Introduction

Continuous compliance monitoring is the practice of monitoring organizational transactions in real-time. While the concept of continuous monitoring is not new, the ability to do so with the help of advanced analytics and algorithms has dramatically improved in recent years.

Continuous monitoring has many benefits and helps organizations to reduce risk by enabling the following:

1. Automated risk scoring
2. Focusing on high-risk transactions
3. Leveraging AI and Machine Learning
4. Continuous program improvement
5. Data-driven decisions

This white paper will examine these methods of reducing compliance risk and other considerations for organizations when implementing these strategies

1. Automated risk scoring

While many compliance programs devote most of their resources to front-end approvals and due diligence, automated risk scoring of employee expenses and vendor and customer financial transactions can continuously reduce risk by focusing attention on behavior after the initial approval and onboarding process. Ongoing risk scoring ensures that organizations can stay on top of suspicious activity throughout their relationship with customers, vendors, and employees and reduce the overall lifecycle risk.

Risk scores determine the level of risk a third party or transaction poses. Data-driven risk scoring provides compliance teams with objective information about potentially fraudulent or otherwise suspicious transactions that warrant further review. Risk scoring typically involves taking multiple data points and layering multiple analytics using that data to assess aggregated risk across multiple dimensions.

Aggregating these risks, along with factors curated for the company's specific risk profile, makes for a robust and targeted risk methodology that compliance professionals can harness to protect the business.

Effective anti-corruption technology has a methodology for identifying high-risk transactions which can be weighted based on an organization's industry, business model, country risk exposures, and past and present organizational issues. When weighted by importance, those scores efficiently pinpoint areas of high risk. It becomes much harder for counterparties or employees to evade the algorithm when multiple risk analyses are combined across multiple dimensions.

Risk-scoring all aspects of a transaction and providing an aggregated risk score makes it possible to identify hidden risks that subjective and sample-based audits might be unable to locate easily. A robust compliance monitoring solution should weigh transactions and aggregate the scores based on the weighting of multiple dimensions. Having a scoring formula that is too rigid may lead to false positives, false negatives, and inaccurate overall scores. Each analysis should be conducted via numerous methods, including behavioral, statistical, and policy-based analyses, to ensure the review looks at each transaction through multiple lenses.

This process can be made even more efficient by implementing continuous monitoring methodology and technology, which can automate data ingestion and risk scoring and provide results in real-time instead of in snapshots of a specific period. Such an approach can result in a daily or weekly escalation of risk-scored transactions for internal compliance, audit, and monitoring teams to review.

2. Focusing on high-risk transactions

Traditional auditing and monitoring efforts are manual and control-focused and tend to generate too many items to review. The same transaction may be sampled multiple times if it appears in results from different tests. This approach is often inefficient and ineffective, failing to connect the dots between numerous risk indicators for a specific transaction.

Many companies do top 10 or top 20 lists of different spend categories or in different vendor categories. For example, many compliance and audit teams focus on lists of the top travel and expense spenders in their company, but that might confirm that the CEO has the highest T&E every month, which isn't very informative.

Looking at the top 10 or 20 is a start that can only get you so far. Spend amount is just one of many factors of risk that should be examined simultaneously to surface your highest risk behavior. For example, your highest-risk vendor in the customs broker category might be in the middle of your spend distribution. However, if the broker's invoice payments are frequently expedited, paid to an offshore bank account, always in round values, their address matches an employee's home address, or a combination of these factors, the transaction should be flagged as high-risk. Multi-dimensional risk analysis using multiple data sets is how compliance data analytics helps compliance teams to focus their efforts on high-risk transactions.

Compliance monitoring prioritizes your efforts within the monitoring of spend and revenue data by displaying the full context of the transaction and its risk results together so that you can focus on the risk of a transaction holistically.

Since the risk score is calculated at an aggregated level across multiple analytics, compliance professionals can prioritize transactions for review based on the company's unique risk profile.

3. Leveraging AI and Machine Learning

Fraud and other suspicious behavior is often not easy to detect with simple random sampling. While it may be effective for detecting consistent issues across data populations, fraud is generally not detected in this manner. Using the sampling approach may not quantify the full impact of control failures or accurately estimate them within a specific population. Because a small anomaly might not seem significant at first glance, it may be overlooked. As time goes on, that small anomaly might result in significant fraud. All relevant transactions must be assessed to effectively focus the efforts and impact of compliance for the organization. However, assessing thousands or more transactions is an insurmountable task without the right technology.

New advancements in technology for compliance enable companies to leverage Artificial Intelligence (AI) and Machine Learning (ML) to automate the analysis of large volumes of data and build tailored algorithms based on organization-specific risk. Integrating AI/ML into a compliance program is the best way for compliance professionals to reduce risk and ensure that their systems deliver increasingly accurate and targeted results over time. A continuous monitoring risk-scoring platform, in particular, can benefit from machine learning by providing feedback on the risk-scored transactions to improve the system's analyses, ensuring more accurate results as the system continues to learn.

Implementing an effective AI/ML system can be easier said than done, especially if a company chooses to build a custom solution. Building an effective AI/ML system from the ground up requires extensive coding knowledge and skilled data scientists who will need to improve the system iteratively. Without the proper foundation and updates, the algorithm may not learn from its mistakes, which defeats the point of using an AI/ML system.

A better solution for leveraging AI and ML is to purchase and customize off-the-shelf software. Compliance software that can run spend data, from enterprise spend systems to libraries of fraud analytic tests typically used by forensic accountants during investigations, already exists. When researching the type of software that is right for your business, be sure to select a solution that enables users to configure risk analytics via a no-code user interface. Compliance teams shouldn't need specialized skills or the expertise of data scientists or engineers to set up or manage the software

4. Continuous program improvement

An effective compliance program is regularly reviewed, adapted, and improved in light of new data and trends. Ongoing monitoring based on objective data can identify areas of potential non-compliance, and resulting areas of program improvement, in real time and more rapidly than short-term evaluations and assessments. Not only does this save companies time, but it also enables them to incorporate any findings into their analytics model. Incorporating findings helps compliance teams reduce risk by preventing future occurrences and improving the compliance program's overall health and effectiveness while keeping it in line with the expectation of enforcement agencies like the U.S. Department of Justice to have a system in place for immediate detection and remediation.

When assessing your program for improvement, consider the most common fraud schemes and those specific to your company's risks. Your investigative lens should re-examine how controls are implemented and whether they are working properly. Look for controls not managed by application control settings and controls that do not function properly. Investigate patterns and fraud indicators identified through fraud detection testing, continuous auditing, and monitoring.

Continuous compliance monitoring facilitates rapid compliance program improvement by making real-time data available for compliance professionals. For example, if a whistleblower allegation comes through the compliance hotline, Compliance and Investigations professionals can quickly pull up risky transactions for that individual, vendor, customer or country. Instantaneously, companies can start changing their analytics to detect new transactions that fit the new pattern. If a new red flag is identified in the media for an existing vendor, that vendor can quickly be added for additional monitoring. All of the transactions from that vendor can be monitored in real-time. If certain transactions are of interest, for example, consulting expenses charged by a distributor, those transactions can be targeted for additional scrutiny.

Continuous compliance monitoring and data analytics help companies to reduce risk by rapidly identifying areas of program improvement. Findings can be incorporated into the analytics models, program controls, and scoring algorithms to prevent future occurrences and improve the program's overall health

5. Data-driven decisions

The use of data to support business strategy and decision-making is nothing new. For decades, business functions like marketing and sales have used data insights to assess, predict, and capitalize on revenue growth opportunities. 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.

Hotline reports have long been a key detection tool when it comes to detecting fraud. Yet frauds detected in this way mean any related data tend to be historical (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 uses 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 much earlier or even prevent them from occurring.

Contextual analytics refers to the layering and connecting of different data sets, such as various transactional data sets within an organization, which provides meaningful context to identify risk. This process is directly integrated into a data-driven compliance program and does not require compliance or audit professionals to contextualize the data manually. For example, a pre-approval system in a corporate compliance program powered with contextual analytics can view a request for funds and compare it to similar requests or requests by the same recipient to determine if the requested payment is a non-compliant outlier. Similarly, a third-party spend monitoring process can consider third-party due diligence results to provide further context around risk with that particular spend item.

As its name suggests, contextual analytics can provide organizations with actionable insights based on their organization's data, rather than just presenting raw data sets without clarifying what the information in those data sets means in a broader context.

However, a data-driven compliance program can run deeper analyses that provide insightful context about the effectiveness of an organization's compliance processes. For example, consider traditional pre-approval processes, which are typically manual and paper-based. In a data- driven program, a compliance professional could review a pre-approval request to host a meeting by examining the request in the context of other meeting requests to determine if the amount of the desired spend per recipient is an outlier. Another example of how contextual analytics can bolster a compliance program is via due diligence. If a compliance professional with a data-driven program reviews a due diligence request to engage with a third party, they can access monitoring results to determine if any historical transactions with that third party have been suspicious or contrary to policy. This contextual information can help compliance professionals make informed decisions based on concrete data.

Using data in compliance isn't just about satisfying the prosecutors if and when you get in trouble. It is about compliance demonstrating value to the rest of the company every single day. Yes, using data analytics is in line with U.S. Department of Justice expectations and can help companies avoid expensive and reputation-damaging enforcement actions. More importantly, compliance teams that use business data can uncover everything from fraud to waste and inefficiencies in the company's use of resources. When compliance data analytics identifies issues such as duplicate vendors or invoices or paying vendors too quickly, compliance can quantify its contribution to the company's bottom line.

Once compliance data analytics are implemented, functions beyond compliance across the enterprise can benefit. Internal Audit teams can reorganize their efforts to focus less on labor and cost-intensive periodic sample-based audits to leverage more comprehensive data analytics and do deeper forensic reviews and third-party audits based on the data analytics findings. The Investigations team can access real-time data – risk-scored transactions for vendors and employees – without having to reach out to IT and Finance. They can scope and resolve their investigations far more quickly and satisfy the ever-present demands of the business leadership for faster close-out of investigations.

The Finance and Procurement organization can use the same data analytics to review existing and new third-party engagements and rationalize the vendor base to reduce the risk for the organization. Business leadership can have real data showing them their spend and risk and feel more empowered to decide whether the money they are spending is justified by the risk posed. Compliance teams often talk about shifting accountability for compliance to the business - for them to "own their compliance." What better way to do that than to give the business the tools to do just that - actual risk data for their teams' financial transactions?

Conclusion

The June 2020 update to the DOJ's Evaluation of Corporate Compliance Programs guidance (2020 Guidance) emphasized that corporate compliance programs must be updated and capable of delivering actionable insights on an ongoing basis. The 2020 Guidance specifically notes that companies should focus their resources on monitoring high-risk areas. More recent statements from the DOJ have pushed the expectations further to require companies to have systems to immediately detect, investigate and remediate non-compliance. A data-driven compliance program empowers organizations to achieve these things.

Implementing a data-driven compliance program will not magically root out every potential bit of fraud, corruption or other wrongdoing in an organization overnight – but this is where risk scoring and machine learning shine. A well-built system is fed risk scores on an ongoing basis, which machine learning can use to ensure that the system produces more accurate analyses uniquely tailored to an organization over time. A program capable of automatically aggregating risk scores can detect suspicious transactions that may otherwise go uncovered and ensures that compliance experts can focus on the highest risk issues that require manual intervention.

One-on-One Advice

Our team of experts has implemented Case IQ for compliance teams around the world.

They are available - free of charge - to speak with you and share the best practices we've learned. No pushy salespeople, just a chance for you to learn from our experts.

With our suite of compliance tools, reporting hotline, and case management software, plus a 25-year track record of successful implementations, Case IQ is the global leader for end-to-end compliance risk management. To get a demo please visit www.caseiq.com/request-a-demo.

To book your one-on-one, please contact:

(800) 465-6089

sales@caseiq.com
media@caseiq.com
support@caseiq.com

300 March Road
Suite 501 Ottawa,
Ontario K2K 2E2
Canada

DON'T MISS OUT
Visit CaseIQ.com for more great investigation resources.