Implementing Technology to Prevent or Resolve an Enforcement Action

Case IQ

Introduction

When reviewing an organization's compliance program, the primary consideration of enforcement agencies, such as the U.S. Department of Justice, is not how complex the program is by design or how much it costs to maintain. Their primary consideration is whether the program is effective, meaning is the program capable of consistently preventing non- compliance and detecting it immediately if it does occur, stopping further non-compliance. Organizations that have enacted strong controls to prevent and detect misconduct can benefit tremendously from this investment should a violation occur.

Regulatory expectations for effective compliance programs continue to increase steadily. This trend has caused compliance professionals and executives within organizations to continually re-evaluate the effectiveness of their compliance programs. These program assessments often highlight the inadequacies of many traditional compliance processes. The days of infrequent, sample-based audits or periodic hotline reports (that may only surface issues months or years after misconduct occurred) are no longer sufficient to meet regulatory expectations. Compliance modernization is of paramount importance for organizations seeking to satisfy regulatory expectations and proactively combat non-compliance.

Implementing technology is one of the avenues organizations can take when modernizing their compliance programs. Programs that utilize technology are more efficient, cost- effective, and capable of immediately detecting suspicious activity in a fraction of the time compared to traditional compliance processes. Technology is particularly impactful for organizations seeking to resolve matters related to financial crimes, such as corruption, fraud, or kickbacks. Software solutions can streamline the processes of maintaining accurate books and records, while transaction monitoring tools can aid organizations in proactively detecting bribes or other forms of financial corruption.

It is essential for organizations to understand why traditional compliance processes are no longer sufficient and the specific ways that technology can aid compliance departments. This paper will break down each of these points and outline how technology can bolster an organization's compliance program and help to prevent or resolve an enforcement action.

Traditional Compliance Processes & Metrics Are No Longer Sufficient

Data has long been a part of compliance programs, but traditionally, compliance teams have only used somewhat superficial processes and metrics to gauge the effectiveness of their programs. Numbers regarding the completion of training or Code of Conduct certifications, hotline and investigation statistics, and the number of third parties that have completed due diligence are important elements to understand. However, none of these data points can answer whether a compliance program effectively mitigates risks with any level of confidence.

For example, an organization may have a low number of hotline reports in a given year, but that does not necessarily mean that non-compliance is not happening. Without additional data, it could mean that the organization has fostered a culture of fear of retaliation that has dissuaded employees from reporting such activity. Another example would be an organization that reports a high training completion rate. A high percentage of mandatory ethics and compliance training course completions does not guarantee that employees follow the training or will even understand its practical application when faced with a high-risk situation.

The U.S. Department of Justice has repeatedly emphasized that compliance programs need to work in practice and deliver meaningful insights rather than merely providing surface-level information such as the examples above. The Department updated its guidance for compliance programs in June 2020 and outlined three key questions that prosecutors should ask when evaluating programs:

1. Is the corporation's compliance program well designed?
2. Is it adequately resourced and empowered to function effectively?
3. Does the compliance program work in practice?

Since the 2020 guidance, the Department of Justice has refined its thinking further in a manner that has only heightened expectations on organizations. In public remarks in March 2022, Assistant Attorney General, Kenneth A. Polite, stated: "[A]s a former Chief Compliance Officer who now serves as the head of the Criminal Division, I want to know whether you are doing everything you can to ensure that when that individual employee is facing a singular ethical challenge, he has been informed, trained, and empowered to choose right over wrong. Or if he makes the wrong choice, you have a system that **immediately detects, remediates, disciplines, and then adapts to ensure that others do not follow suit** [emphasis added]."

The hallmark of a compliance program that is well-designed, adequately resourced and empowered, and working in practice is now whether it can immediately detect, remediate, and discipline, such that the same violation does not occur again. Traditional compliance programs are ill-equipped to meet this standard.

The traditional reliance on hotline reports and periodic sample-based audits is insufficient to meet this standard. As outlined in the Association of Certified Fraud Examiner's 2022 Report to the Nations, problems reported via hotlines are only uncovered, on average, 12 months after the fact—a far cry from "immediate," and by which point the non-compliant activity could already have been repeated. Beyond these timing limitations, hotline reports require employees to report wrongdoing, and audits require choosing the right audit targets and samples—both of which limit the reach of these tools to effectively measure non-compliance.

These limitations are exacerbated when it comes to preventing and detecting financial non-compliance, such as bribery, fraud, or kickbacks. Such risk can appear in a small number of transactions among millions for an organization within the space of a year. Compliance officers often have insufficient access to this broader financial data set and few tools to analyze risk within that data. The Department of Justice wants to know whether organizations can identify compliance violations immediately within this data, and most compliance teams today would fall far short of meeting that expectation.

Implementing Technology Can Help Organizations Prevent or Resolve Enforcement Actions

Implementing technology into a compliance program will boost the program's efficiency, accuracy, and overall ability to prevent and detect suspicious activity proactively and in real time.

For example, let's consider how difficult it can be to detect bribery manually. Such violations are often hidden in otherwise legitimate-seeming contracts or employee expenses that likely have passed through myriad company processes, such as Procurement or expense reimbursement tools. The scale of transactions and the nature of obfuscation involved make manual detection particularly difficult.

However, a technology-driven compliance system could involve pre-approval tools that subject these expenditures to heightened risk-based review alongside transaction monitoring software that deploys forensic data analytics tools on 100% of expenditures across an organization's financial systems to detect anomalous transactions. The result would be a comprehensive review of risk, leading to a much higher degree of confidence in terms of the level of true non-compliance within the organization and a greater ability to immediately detect issues. Ultimately, such a technology- enabled compliance program would be much more effective.

Implementing technology into your compliance program also shows enforcement agencies that your organization is committed to effective compliance and seeks to implement a control environment that reinforces and rewards ethical behavior.

Prosecutors and regulators know that even the most advanced compliance systems will be unable to eliminate all non-compliance, and rogue employees will always present a risk. Still, they are willing to give credit to organizations that have made concerted efforts to prevent such activity. If your organization has made that effort prior to finding itself in front of the enforcement agency, the agency is far likelier to consider the program well- designed and effective and place the blame for non- compliance on rogue actors rather than the organization.

In addition, technology-driven systems that assess wide-ranging data from your financial systems for risk can drive additional compliance program operational benefits. For example, if your organization risk scores all third- party invoices and distributor transactions, that risk data can be aggregated and rolled up. This data can be used to inform country risk assessment comparisons, help with audit planning, highlight areas for additional communication and training, and be democratized and shared with country personnel to embed an overall compliance culture within upper and middle management. Compliance officers can use the insights provided by technology to upgrade their compliance processes more quickly to address the root causes of misconduct. This continuous assessment and improvement process directly aligns with the expectations of enforcement agencies, which emphasize the importance of continually testing and iterating compliance programs to ensure they are sustainable and able to adapt to changing risks.

Crucially, implementing technology into a compliance program ensures that organizations do more than take a basic “tick-the-box” approach to their compliance processes. Enforcement agencies expect Chief Compliance Officers to demonstrate knowledge and ownership of their compliance programs, while the compliance officers on their team should be empowered to follow suit. Organizations that have compliance programs that can actually detect and mitigate fraudulent activity—by using the technology-driven tools described above—will be better positioned to resolve their enforcement actions favorably and avoid having monitorships imposed on them.

Technology Provides Organizations With Powerful Tools to Detect Violations

Compliance systems that run on modern technology boast several features that are invaluable in detecting non-compliance, such as bribery, fraud, or kickbacks. For example, high-tech compliance systems can apply forensic data analytics to the entirety of an organization's T&E expenses, invoices, rebates, and other financial transactions to risk score those transactions and ensure that compliance officers have an accurate and all-encompassing view of spend risk across their organization. Such compliance systems can subject any given transaction to dozens of statistical, behavioral, and rule-based analyses and automatically assign aggregated transactional risk scores, ensuring that high-risk transactions can be easily detected and singled out for review. This analysis ensures that compliance officers focus their limited time and resources on high-value activities rather than attempting to comb over the entirety of their organization's data manually.

Consider a case where a multinational conglomerate's compliance team suspects that one of the organization's sales teams within a market is violating anti-corruption laws, such as the FCPA or Sapin II, by bribing a foreign government official. If the compliance team had transaction monitoring software, the software would automatically escalate anomalous transactions for review in real time from that office to determine whether wrongdoing has occurred.

To be clear, technology does not replace the need for skilled compliance officers. Instead, it can automate many time-consuming tasks and serve as an aid for compliance teams to ensure more efficient and targeted use of their time to identify and remediate true non-compliance.

Without such technology, the compliance team may never be aware of an issue or, if they are made aware, may have to physically travel to the office and manually sift through the underlying raw financial data to identify the problematic transactions.

Another significant benefit of compliance technology is the continuous nature of its monitoring. The Department of Justice expects organizations to effectively manage risk across the lifespan of their relationship with any given entity, particularly with third parties. For example, a third party designated as low risk during the initial due diligence process may have been misclassified, or their scope of work may change throughout the relationship. Changes in circumstances of a third party after onboarding could position them to violate anti-corruption laws, such as the FCPA or Sapin II, which continuous monitoring technology would be able to detect.

Furthermore, manual audits, which are infrequent and prone to human error, may fail to detect violations and other issues. If they are eventually identified, such detection may only occur months or even years after the activity has begun. At that point, it may already be systemic.

Technology empowers compliance teams to detect wrongdoing in a fraction of the time. Thanks to automatic risk scoring and forensic data analytics, those insights will be more accurate and backed up by meaningful data.

Implementing Technology Helps Organizations Satisfy Regulatory Expectations

We have discussed how traditional compliance processes can fail to satisfy enforcement agency expectations for compliance programs. Now, let's consider how implementing technology into a compliance program can help organizations meet regulatory expectations related to potential fraud, corruption, and kickback cases, such as those related to the FCPA, Sapin II, the U.K. Bribery Act, or the U.S. Anti-Kickback Statute.

One of the key factors in the Department's compliance program evaluation is determining whether it is actually working and functioning effectively in practice. For example, when evaluating a compliance program, the Department of Justice expects organizations to be capable of continuously testing the compliance program's effectiveness. The Department also emphasizes that effective programs should be able to detect and remediate issues immediately. Prosecutors consider the responsiveness of a compliance program to be of paramount importance. Programs that immediately detect and allow for the remediation of issues and are able to adapt to ensure that others do not commit similar misconduct receive particular credit from prosecutors.

Additionally, integrating technology into your compliance program can help your organization avoid the imposition of an independent monitor. The Department of Justice may consider bypassing a monitorship on organizations that have made a concerted commitment to implementing a robust compliance program. It is vital that the organization has demonstrated that its controls are effective and can be regularly updated to adapt to changing risks.

An organization that is able to test its controls continuously and verify that those controls are effective is in a better position to avoid a monitorship. The benefits of a technology-driven compliance platform are ideally suited to help organizations satisfy all of these regulatory expectations.

The Department of Justice's Criminal Division prosecutors already use data analytics to detect and combat criminal schemes domestically and internationally. The Department expects organizations to do the same thing and consider what data analytic tools they could use to monitor compliance with laws and policies to ferret out wrongdoing.

Off the Shelf Systems Can Allow Organizations to Quickly and Effectively Implement Technology

The benefits of integrating technology into your organization's compliance processes are myriad, but organizations don't need a team of data scientists and engineers on the payroll to begin implementing such technology. Innovative and user-friendly off-the-shelf compliance software can empower organizations to quickly implement cutting-edge compliance solutions that will satisfy regulatory expectations.

Organizations can implement off-the-shelf compliance technology more quickly and cost-effectively than attempting to build software in-house. Furthermore, compliance technology from specialized vendors is built around best practice requirements. It is designed to be adaptive, ensuring that your organization's compliance processes are sustainable and capable of adapting to changing risks and regulatory expectations.

In addition, off-the-shelf compliance technology is designed to be accessible. Software from leading compliance vendors does not require specialized data skills to operate. This ease of use ensures that your organization's compliance teams and senior management will be able to demonstrate knowledge and ownership of their organization's risk data and overall compliance program.

The Next Step

Compliance has not traditionally been viewed as a technology-driven discipline, but the use of high-tech tools has become increasingly popular among organizations seeking to be proactive in their fight against fraud and corruption. Lextegrity (a Case IQ company) was founded on this concept by a team of former in-house compliance and audit professionals who wanted to build the kind of software that they wished they had while they were working in-house. The workflow automation and data analytics tools provided by platforms such as Case IQ can help organizations better understand and immediately prevent and detect risks across their enterprise and ensure that their compliance processes are in-line with regulatory expectations.

In fact, our product has been selected by multiple organizations looking for help to resolve enforcement actions and was even cited by the U.S. Securities & Exchange Commission as an important tool in one company's remediation of bribery issues. When considering whether to implement technology into your compliance program, another resource that can help your consideration is How to Measure the Effectiveness of Your FCPA Compliance Program.

Taking the technological step forward can seem like a significant leap for organizations that are still relying on traditional compliance processes and metrics, but the opportunities to transform your risk management processes through technology are more accessible than ever.

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.