DOES YOUR FRAUD RISK MANAGEMENT PROGRAM ACTUALLY WORK, IN PRACTICE?

Global anti-fraud and compliance enforcement is on the rise, and regulators want proof that fraud risk management programs are effective. Here we look at some of the hard questions organizations need to ask and some examples of how companies have updated their systems to tackle fraud in the post-COVID environment.

As the new year dawned, Susan felt good about what she and her team had accomplished in 2021 with their fraud risk management program. As the head of internal audit and investigations at a mid-sized manufacturing company, she was confident her program aligned to the five principles described in the ACFE/COSO *Fraud Risk Management Guide* (FRMG). (See ACFE.com/fraudrisktools.) But now, a few months into the new year, Susan is struggling to find a solid, data-driven answer for her chief compliance officer and chief financial officer, who are asking how the program is actually working, in practice.

Supply-chain issues, new hybrid working models (with many employees working remotely) and other changes to the business environment brought on by the COVID-19 pandemic have altered her company's fraud risk landscape. How can Susan ensure her program is relevant; and, even more important, how can she and her team measurably demonstrate anti-fraud and compliance effectiveness via key performance indicators? Susan and her company are fictional, but these are dilemmas currently on the minds of many anti-fraud and compliance professionals and their organizations.

COLUMNIST
VINCENT M. WALDEN, CFE
ALVAREZ & MARSAL'S DISPUTES AND INVESTIGATIONS PRACTICE

Leading guidance provides framework

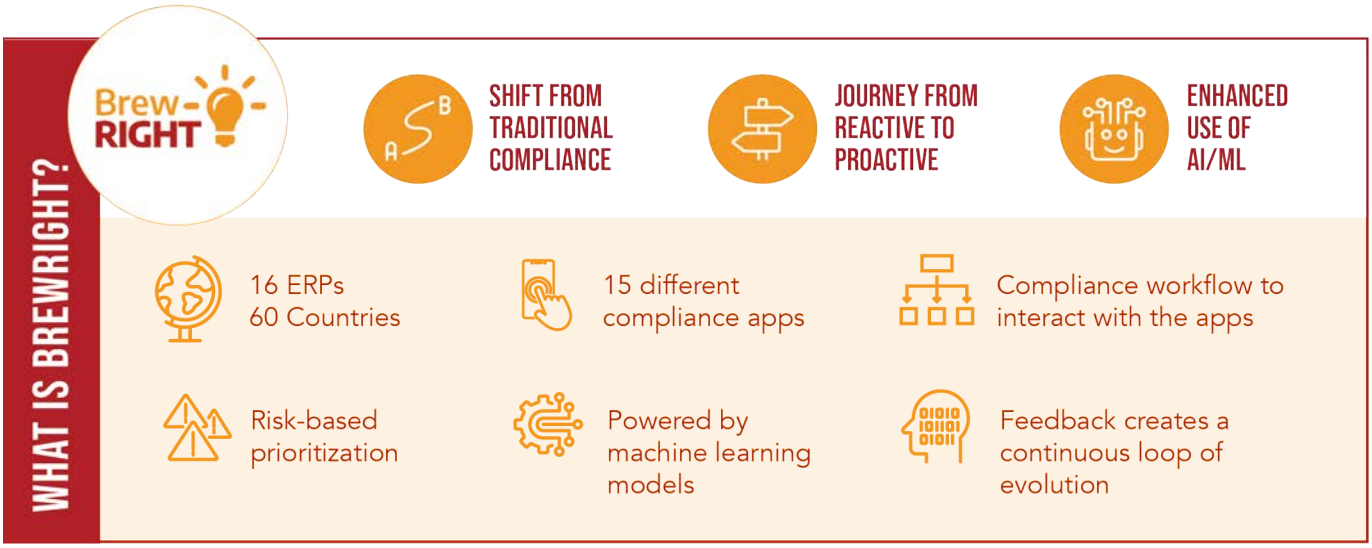
As CFEs, we come from many different disciplines: accounting, internal audit, law, compliance, law enforcement, finance, government and business, to name a few. Each of these disciplines has its own guidance on mitigating fraud risks.

Perhaps best known to CFEs and anti-fraud practitioners is the aforementioned FRMG. COSO's Fraud Risk Task Force is currently updating the FRMG, with an expected release later this year. COSO, short for the Committee of Sponsoring Organizations of the Treadway Commission, generally sets forth the expectations for an effective internal controls environment. (See "Innovation Update," by Vincent M. Walden, *Fraud Magazine*, November/December 2021, tinyurl.com/2p9aft3c.)

In the legal and compliance arena, practitioners often look to the U.S. Department of Justice's (DOJ) "Evaluation of Corporate Compliance Programs (Updated June 2020)," which carries some weight as it's what prosecutors use, in part, to decide on an offending organization's culpability and potential penalties. (See tinyurl.com/yyw9lcc2.)

Kara Brockmeyer, a partner with Debevoise & Plimpton LLP and former chief of the SEC Enforcement Division's FCPA Unit, advises clients on how to improve their anti-fraud and anti-corruption programs and points to 10 key questions from the above DOJ guidance. I've collaborated with Brockmeyer in the past to organize some of the DOJ guidance's key questions that focus on how organizations can measurably demonstrate the effectiveness of a compliance/anti-fraud program. She's summarized them on page 13. As you read them, ask yourself: "How well can my organization answer these questions?"

CATEGORY	DOJ'S QUESTION
Risk assessment	"Is the periodic review limited to a 'snapshot' in time or based upon continuous access to operational data and information across functions?" (Based on page 3 of DOJ guidance.)
Risk management	"What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?" (Based on page 3 of DOJ guidance.)
Incorporating lessons learned	"Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned, either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?" (Based on page 4 of DOJ guidance.)
Adequate resources and results tracking	"How has the company collected, tracked, analyzed and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weakness? Does the company periodically test the effectiveness of the hotline; for example, by tracking a report from start to finish?" (Based on page 7 of DOJ guidance.)
Third-party management	"Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks by third-party partners; including the third-party partners' reputations and relationships, if any, with foreign officials." (Based on page 7 of DOJ guidance.)
Third-party management	"Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?" (Based on page 8 of DOJ guidance.)
Third-party management	"Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date?" (Based on page 8 of DOJ guidance.)
Data resources and access	"Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?" (Based on page 12 of DOJ guidance.)
Continuous improvement, periodic testing	"Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?" (Based on page 16 of DOJ guidance.)
Analysis and remediation - transactions	"How was the misconduct in question funded (e.g., purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?" (Based on page 17 of DOJ guidance.)
Policies and procedures	"Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?" (Based on page 4 of DOJ guidance.)



Source: AB InBev

Going back to our fictional example, Susan evaluated her own organization in the context of the DOJ questions on page 13 and found many couldn't be fully answered. This was especially a concern with respect to how her company conducted risk assessments and managed third parties. For example, her company conducted extensive due diligence on third parties during the vendor setup process. However, risk indicators, such as contract terms or thresholds for spending were never migrated into the financial accounting system that actually paid and tracked those vendors.

Don't overlook in-house resources

Fortunately, there's hope for Susan — and others in her position looking to measurably demonstrate an effective compliance and anti-fraud program. If you have a marketing department, finance department, information technology team or some other business function where the analysis of data requires them to utilize business intelligence, data warehouse or data visualization tools to help them make decisions, you may be able to leverage what's already in place — without buying expensive software licenses or data warehouses. Whether those resources require major or minor modifications is typically based on the nature and complexity of the business. But in my experience working with a variety of clients in several industries, there are always some "quick-hit" wins and/or cloud-based solutions that you can rapidly deploy to improve transparency and address key fraud risks.

Here are examples of how some organizations are improving and updating their compliance and fraud risk management programs.

Amy Kulikowski is vice president, internal audit for Cooper Standard, a global supplier of sealing and fluid handling systems in transportation and industrial markets. Her team uses scripting (i.e., a programming language that automates certain tasks) and other self-operating tools with their financial accounting/enterprise resource planning (ERP) system to refresh monthly and quarterly data on all global procure-to-pay and T&E spending. Hosted on a secure, third-party, cloud-based analytics platform, their fraud risk management and compliance-monitoring system assesses and monitors hundreds of thousands of payments each month, and ranks thousands of vendors and employees from highest to lowest risk based on over two dozen risk criteria.

Patricia Bradford is chief human resource officer at Elara Caring, a national skilled-home-healthcare, hospice care and personal-care-services organization. She uses scripting and automation tools to gain better insights into her organization's employee payroll base by integrating over 1,200 distinct payroll files of over 25,000 full- and part-time employees. Working with her IT department and an outside consulting firm, Bradford leveraged the business intelligence tools already used in her organization to build dynamic, risk-scoring and anomaly detection dashboards that flag payments to terminated employees, statistically anomalous payments, potential overtime abuses, repeated hiring and termination patterns and off-cycle disbursements, among many other data-driven tests.

On a larger scale, who would've thought that the world's biggest beer brewer also has one of the most mature anti-fraud and compliance-monitoring platforms? There isn't enough room in this column to describe how Anheuser-Busch InBev uses in-house resources

across its IT, data science, finance and legal departments to improve transparency in its businesses through its BrewRIGHT platform, but I encourage you to read more in The Wall Street Journal and Harvard Business Review. (See "AB InBev Taps Machine Learning to Root Out Corruption," by Dylan Tokar, The Wall Street Journal, Jan. 17, 2020, tinyurl.com/d4abch3k; and "Designing a Compliance Program at AB InBev," by Eugene Soltes, Harvard Business Review, March 28, 2018, tinyurl.com/2eta33x4.) For a visual primer, Dheeraj Thimmaiah, global director, ethics & compliance at Anheuser-Busch InBev, provides a summary of how the BrewRIGHT platform works globally. This is integration and data transparency at its best. (See graphic on page 14.)

Make an impact this year

Regardless of your organization's size or complexity, it's important to bring transparency to your business, especially around company spending and/or sales. This is true not just for regulators — who are increasingly clamping down on organizations out of compliance — but for sustainability and business performance. As you think about your goals for this year and next, consider how you can partner with other areas in your organization to measurably demonstrate that your fraud risk management program actually works, in practice. ■ FM

Vincent M. Walden, CFE, CPA, is a managing director with Alvarez & Marsal's Disputes and Investigations Practice and assists companies with their anti-fraud, investigation and compliance monitoring programs. He welcomes your feedback. Contact Walden at vwalden@alvarezandmarsal.com.