DOJ ASKS, 'CAN YOU SHOW YOUR COMPLIANCE AND ANTI-FRAUD PROGRAM ACTUALLY WORKS?'

The U.S. Department of Justice (DOJ) recently updated its "Evaluation of Corporate Compliance Programs," the primary guidance for DOJ prosecutors when they assess penalties. These updates provide insights into the factors DOJ is likely to emphasize when it evaluates the effectiveness of your organization's compliance program — should you come under scrutiny.

The Evaluation of Corporate Compliance Programs (tinyurl.com/yyw9lcc2), originally published in April 2019 and updated in June, is the U.S. Department of Justice's (DOJ) leading guidance on how its prosecutors evaluate the design, deployment and effectiveness of companies' compliance programs.

Many elements in the DOJ guidance echo the *COSO/ACFE Fraud Risk Management Guide* (tinyurl.com/y96nsyl8). However, the DOJ document is also a handbook for prosecutors when they're deciding on whether to charge companies with violations of laws. The guidance also helps them develop sentencing recommendations or assign corporate compliance obligations, such as naming independent monitors to oversee improvements of compliance programs. This guidance document gives you a unique look into how DOJ prosecutors could view and evaluate your organization's compliance program.

The 2020 DOJ guidance emphasizes that companies can't use a one-size-fits-all approach when they construct their compliance programs. The guidance also asks prosecutors to make a "reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape and other factors, both internal and external to the company's operations, that might impact its compliance program."

The 2020 updates aren't dramatically different from the original April 2019 document, but they signal that prosecutors will be looking more closely at whether compliance programs: 1) are adequately resourced 2) have formalized processes in place to continuously improve their effectiveness 3) have effectively incorporated the use of data analytics.

Adequate resources

Unchanged from the 2019 guidance are three fundamental questions DOJ asks, which set the tone for the entire document:

- "Is the corporation's compliance program well designed?"
- "Is the program being applied earnestly and in good faith?" (In other words, is the program adequately resourced and empowered to function effectively?)
- "Does the corporation's compliance program work (in practice)?"

DOJ instructs prosecutors to probe specifically whether a compliance program is simply just a "paper program" or is "implemented, reviewed and revised, as appropriate, in an effective manner."

The revised guidance also asks if a company has adequately invested in training and development of compliance personnel and, as we'll discuss further in this column, whether the compliance function has access to data that it can monitor and test.

During challenging economic times, companies might be tempted to first cut non-revenue-generating functions like compliance and investigative departments, which they can wrongly perceive as liabilities not assets. However, declining bottom lines also increase opportunity and pressure to commit financial and economic crimes. The updated guidance suggests that DOJ already perceives that companies aren't adequately funding many programs. So, further compliance cuts could increase risk.

Continuous improvement

The overall effectiveness of a compliance program is still a primary consideration of DOJ's analysis. But the guidance suggests that prosecutors will be more focused on companies establishing formal processes to continually evaluate and update their compliance programs.

Prosecutors will want to see continual internal evaluations plus formalized approaches, which will generate hard data and information that will demonstrate measurable compliance. For example, it's not enough for companies to simply update policies and procedures in light of "lessons learned" — an important concept in the guidance. Instead, DOJ now asks if an organization's internal review of its compliance program is "based upon continuous access to operational data and information across functions."

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
MANAGING DIRECTOR, ALVAREZ & MARSAL'S DISPUTES AND INVESTIGATIONS

THE 2020 DOJ GUIDANCE EMPHASIZES THAT COMPANIES CAN'T USE A ONE-SIZE-FITS-ALL APPROACH WHEN THEY CONSTRUCT THEIR COMPLIANCE PROGRAMS.

Other updated sections of the guidance ask if a company publishes its policies and procedures in a searchable format for easy reference and if the company can track those policies that attract the most attention from relevant employees.

Prosecutors will want to see processes for evaluating the effectiveness of compliance trainings and whether employees can easily raise issues and ask follow-up questions. It's no longer enough to simply track who attended a training session and passed a test; prosecutors want to know if a company is evaluating its trainings' impact on employee behavior and operations. (For more on creating effective compliance programs, read my "Innovation Update" column, " 'Profit & Loss-of-One:' Preventing fraud, enhancing compliance using digital twins," *Fraud Magazine*, January/February 2018, tinyurl.com/y2bnp4h3.)

Data analytics emphasis

The updated DOJ guidance specifically emphasizes that organizations need to have access to relevant data sources to allow for "timely and effective monitoring and/or testing of policies, controls, and transactions."

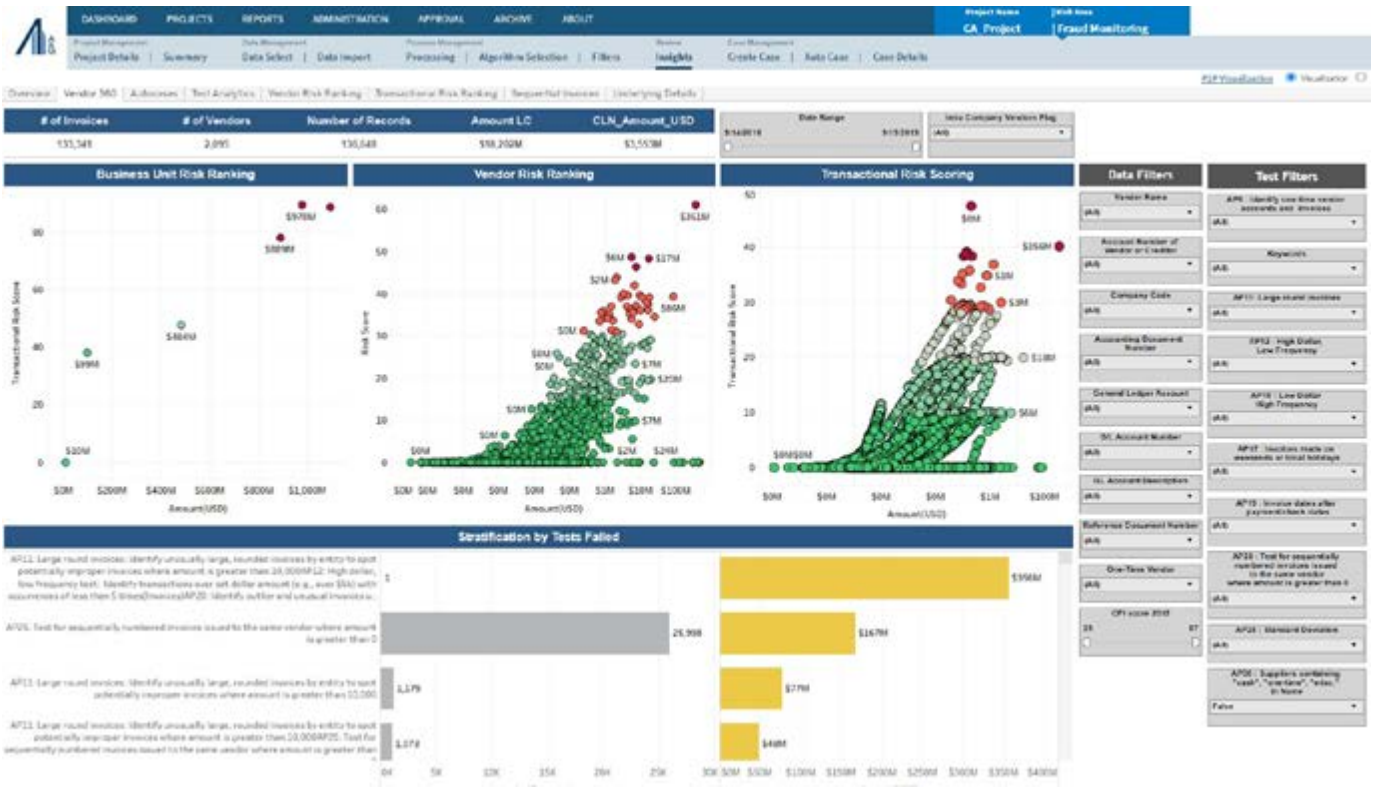
DOJ apparently believes that hard, measurable data and information must be the engines for compliance programs as they already are for most other business processes in an organization such as sales, marketing, human resources and finance. Happy words and vague promises won't cut it. In fact, many of the specific compliance processes that prosecutors will be looking for aren't successful without data transparency — particularly as it relates to analyses of payment streams, such as: 1) payments to vendors 2) employee reimbursements 3) customer sales 4) discounts.

Lagging companies should incorporate forensic data analytics and transaction monitoring into their compliance programs. If you're afraid to dip your toe, recent technology and compliance innovations are greatly easing deployment of analytics programs.

Don't forget fundamentals

Though DOJ guidance emphasizes that hard data must underpin compliance programs, we shouldn't lose sight of the document's fundamental aspects. Overall, the primary goal for a compliance program is to adopt a thoughtful, risk-based approach based on a rigorous and well-documented fraud risk assessment — tenets that fraud examiners have been preaching for years.

The first section of the guidance asks, "Is the corporation's compliance program well designed?" It further describes the fundamentals of an effective compliance program. As you read each of these components, ask yourself what



Sample compliance-monitoring dashboard across multiple business functions

metrics or data you would prepare to demonstrate effectiveness:

- A **risk assessment** that demonstrates that a company understands its "business from a commercial perspective, how the company has identified, assessed and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks."
- **Policies and procedures** that "give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process."
- **Training and communications** designed to "ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees and, where appropriate, agents and business partners." You should be able to demonstrate that the training or communications are risk-based and effective, address misconduct and are readily available to employees.
- **Confidential reporting structure and investigation process** that comprise an "efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers."

"Following the proverb, 'honey catches more flies than vinegar,' companies are quickly shifting from the unfruitful mindset of whistleblowing into the concept of enabling trusted conversations," says Sylvain Mansotte, CEO of Whispli (a company that provides a whistleblowing platform for companies) and a whistleblower himself.

"Organizations are now upgrading their traditional toll-free whistleblower hotlines with more effective and technically advanced forms of secure two-way communications," Mansotte says.

- **Third-party management** that applies "risk-based due diligence to its third-party relationships." Prosecutors will be looking to see if a company engages in risk management of third parties not just at the beginning of relationships but throughout their lifespans. Clearly, DOJ is suggesting that companies shouldn't only be conducting due diligence procedures on third parties

before they do business but also *after* they've signed contracts and they're conducting business and exchanging money.

As shown in the dashboard on page 10, companies can best monitor risk insights by looking at associated transactional activities via forensic data analytics. Data analytics can demonstrate measurable compliance effectiveness and save money by increasing business transparency and stopping rogue payments before they're paid. Use anti-fraud and anti-corruption tests plus behavioral algorithms to detect potentially improper payments. And use risk-scoring procedures to identify your highest risk vendors, customers or employees — by geography, business unit and dollar volume.

- **Mergers and acquisitions** activities that "include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls."

DOJ doesn't want lip service

Ethics and compliance programs have traditionally focused on legal aspects of policies, regulatory requirements, employee training and investigation activities. A compliance or anti-fraud professional traditionally might have collaborated with internal audit and/or procurement functions to introduce financial, data analytics and other due diligence controls, but it would often have been limited to a snapshot in time (as DOJ warns against) and not a continuous process.

Instead of preventing problems, they audited them while they were occurring or after they finished. The audits lacked hard-data underpinning and insights, which disabled preemptive decision making, risk mitigation and improved company performance.

DOJ, with its release of this updated June 2020 guidance, is expecting to see that companies have such components as business transparency practices, continuously improving processes and accessibility to relevant data sources in their corporate compliance programs that measurably demonstrate effectiveness.

How does your program fare? ■ 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 him at vwalden@alvarezandmarsal.com.