WHO OWNS TRANSACTION AND CONTROLS MONITORING?

Who monitors and oversees high-risk transactions in your organization? If it isn't you – an anti-fraud professional – you should heavily ponder this question. In this article, I explore who owns transaction and controls monitoring for vendors, customers and employees. The variety of answers may surprise you.

A common challenge in midsize and large organizations is the false sense of security in thinking that "someone else" or "some other department" owns a particular fraud risk control and has it covered. In reality, the fraud risk perspective of Certified Fraud Examiners (CFEs) is often missing but desperately needed. Let's use finance and accounts payable departments as examples. Who administers and monitors payments to the organization's third parties? As the first line, those in accounts payable often base their risk concerns and perspectives on key internal controls and the presence of approvals, documentation and vendor qualifications required for invoice payment. Are they thinking about anti-corruption risks or fake vendor schemes, conflicts of interest or sanctions compliance? Some of them are, but most of the time accounting staff don't have the bandwidth or background to spot trends, sensitive keywords or patterns indicative of a potentially improper payment or vendor. Oversight is frequently missing from employee travel and entertainment expenses administration. Controls can fall through the cracks in accounts receivable, as well, an area in which commissions, bonuses or discounts are prone to abuse. Are you confident that your organization's financial processes for handling vendors, customers or employees could stop an improper payment or transaction? Let's take a closer look at who owns transactions and controls monitoring in these high-risk areas of an organization.

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
CEO OF KONA AI

As the first line of defense, those in accounts payable often base their risk concerns and perspectives on key internal controls and the presence of approvals, documentation and vendor qualifications required for invoice payment.

A multidisciplinary approach to fraud risk

Fourteen years ago, two of my mentors, Dan Torpey, CPA, and Mike Sherrod, CFE, CPA, examined the value of a multidisciplinary team addressing fraud risk as a "committee," not as a single department. They asserted that leaders across the entire business — executive management, internal investigations, compliance, internal audit, finance, human resources, general counsel and information technology — need to "have a seat at the table." This multifaceted approach, they contended, sets the proper tone at the top for developing fraud prevention policies, communications and training. An effective program also includes a fraud risk assessment, proactive controls monitoring and an effective response plan. (See "Who Owns Fraud? Uniting Everyone to Effectively Manage the Anti-Fraud Program," by Dan Torpey and Mike Sherrod, *Fraud Magazine*, January/February 2011, tinyurl.com/354hnbdn.)

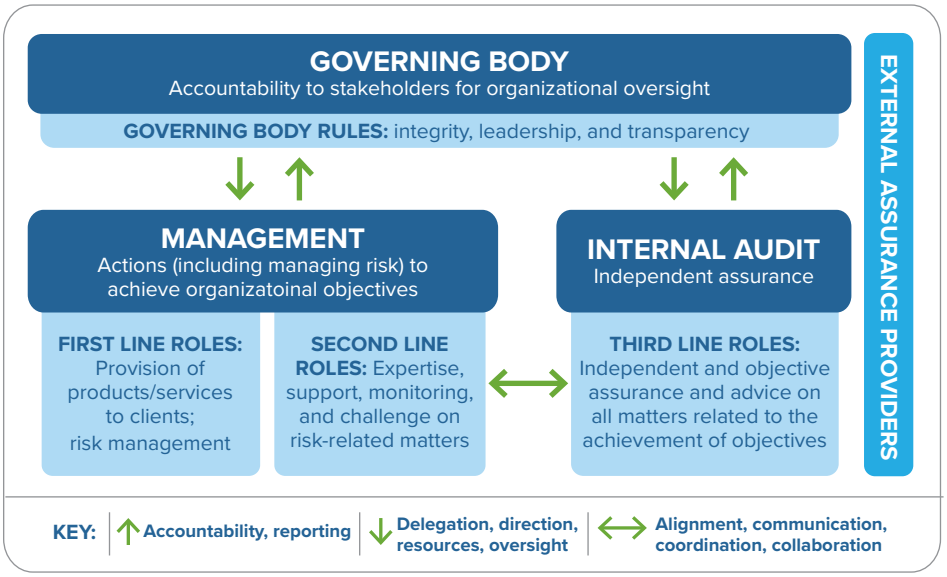
Fast-forward to today's *Fraud Risk Management Guide*, published by COSO and the ACFE, which echoes the same sentiment of a committee approach in the first principle on governance: "Personnel at all levels of the organization have roles and responsibilities with respect to fraud deterrence, prevention, and detection. Board members, internal auditors, compliance professionals, investigators, managers, specialists, and other team members are all important when it comes to fraud risk management." The *Fraud Risk Management Guide* takes it one step further by recommending that one executive-level member of management be assigned overall responsibility for the program: "It is

critical to the success of a Fraud Risk Management Program for one executive-level member of management ... to ensure that the Fraud Risk Management Program is taken seriously and implemented fully. This executive-level person is familiar with the organization's fraud risks and process-level controls and is held responsible for the design and implementation of the processes used to help ensure compliance, reporting, and investigation of alleged violations. It's also appropriate to designate a board member or committee that has overall responsibility for investigating allegations of wrongdoing by members of management." (See ACFE.com/fraudrisktools.) Does your organization have one or two senior-level executives who serve as the chair of your fraud risk management committee?

Three lines model

Drilling down into the responsibility for prevention and detection, Principle 3 of the *Fraud Risk Management Guide* states that, "Fraud control activities are performed at varying levels in the organization and, in some cases, are a combination of both preventive and detective considerations. The range of fraud control activities varies by organization." In the context of the well-known "three lines" concept, The Institute of Internal Auditors (IIA) suggests that the monitoring function is a second-line role. The IIA's three lines concept provides a framework for an organization's risk management approach by entrusting specific responsibilities for risk identification, mitigation and oversight at three levels: first line (management), second line (risk management and compliance) and third line (internal audit). Through independent assessments and reporting to the board of directors, this approach helps organizations protect against fraud and other risks. Specifically, the first line encompasses fraud prevention measures and controls related to daily risks inherent in business processes. In support of the first line, the second line determines emerging risks, designates standards, monitors compliance and devises risk mitigation strategies. The third line independently evaluates the effectiveness of the first and second lines by conducting audits, forming an impartial assessment of the organization's overall risk management framework. (See "The IIA's Three Lines Model: An Update of the Three Lines of Defense," IIA position paper, updated September 2024, tinyurl.com/373fa44z.)

The IIA's Three Lines Model



(Source: "The IIA's Three Lines Model: An Update of the Three Lines of Defense," IIA position paper, updated September 2024, tinyurl.com/373fa44z.)

Whose job is it?

Where do you think transaction and controls monitoring belongs? Is it your job or someone else's? In November 2024, I spoke at the Georgia Chapter of the Association of Certified Fraud Examiners Annual Meeting and polled about 36 CFEs by show of hands. Many agreed that the frontline business was responsible for the initial fraud risk in line with the controls that are in place, with the ability to quickly escalate a problem outside the norm. But almost all agreed that the second line, if not or including the third line internal audit, played a key role in helping design controls and continuous monitoring while providing more of the advanced analytics to find unusual patterns or risks in the data. This would be consistent with a CFE's role in compliance or investigations as a second line.

Compliance indeed takes an active role in proactive monitoring with

respect to setting up the right tools and technologies for effective fraud prevention and detection, according to one of my colleagues who's head of global compliance monitoring at a global technology and manufacturing company. She tells *Fraud Magazine* that collaborating with business unit management (the first line) is essential to maximizing compliance program effectiveness, especially when you can provide the business unit with information or insights that they weren't previously aware of. She says that being visible and engaged with the business has been a key success factor in her career.

A data-driven approach

It's important to arm the frontline business with adequate controls, information, training and risk indicators to assist in fraud prevention and detection, but it's not their main area of focus. The second line — CFEs like you — tasked in oversight functions such as compliance, internal investigations, risk management, legal and finance, are the ones who need to see above the day-to-day operations. As the second line, you're responsible for providing the necessary anti-fraud expertise, support and operations monitoring while also challenging the status quo. Internal audit, the third line, plays a similar role but with greater independence from the business. Policy, training and reactive investigations aren't enough. Effective monitoring and fraud risk management require data to be meaningful to the business and defensible to a regulator. Internally generated data from your own surveys or risk assessments won't suffice. You need actual business data that provides transparency into the operations of the business, including vendors, customers and employees. Such data might include payment and transactional data from your enterprise resource planning (ERP), accounting or due diligence systems or via external data sources. ■ **FM**

Vincent M. Walden, CFE, CPA, is the CEO of Kona AI, whose company mission is to empower compliance, audit and investigative professionals with research-driven, innovative and effective analytics to measurably reduce global fraud, corruption and enterprise risk. He works closely with CFEs, internal auditors, compliance, audit, legal and finance professionals and welcomes your feedback and ideas. Contact him at vwalden@konaai.com.