NONCOMPLIANCE WITH LAWS AND REGULATIONS — CFES' ELEVATED AUDIT ROLE UNDER PROPOSED PCAOB RULES

CFEs, lawyers and auditors — be on alert! The proposed PCAOB's amendments to its auditing standards related to an auditor's consideration of a company's noncompliance with laws and regulations about financial statement audits will have a profound impact on our profession, bringing fraud risk management front and center.

Fraud risk was a top priority in 2023 for the Public Company Accounting Oversight Board (PCAOB), the independent regulatory body established by U.S. Congress to oversee audits of public companies and broker-dealers. The PCAOB is close to ratifying new amendments this summer or fall related to noncompliance with laws and regulations (NOCLAR) that could make legal and investigative professionals, especially Certified Fraud Examiners (CFEs), a critical part of the audit team.

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

The proposed PCAOB changes

On June 6, 2023, the PCAOB proposed amendments to its auditing standards related to an auditor's consideration of a company's NOCLAR in the performance of a financial statement audit to establish and strengthen requirements for (1) identifying, through inquiry and other procedures, laws and regulations with which noncompliance could have a material effect on the financial statements; (2) assessing and responding to the risks of material misstatement arising from noncompliance with laws and regulations; (3) identifying whether there's information indicating that noncompliance has occurred or may occur; and (4) evaluating and communicating when the auditor identifies or otherwise becomes aware of information indicating that noncompliance with laws and regulations, including fraud, has or may have occurred. [See "PCAOB Release No. 2023-003," tinyurl.com/yf7ksnhf.]

In its current form, PCAOB's NOCLAR proposal could expose auditors to increased enforcement scrutiny. Presently, an auditor has no duty to identify illegal acts. However, the proposed amendments to PCAOB's Audit Standard (AS) 2405 would require an auditor to plan and perform audit procedures to identify and assess potential noncompliance. The proposal requires auditors to:

- "Identify the laws and regulations with which noncompliance could reasonably have a material effect on the financial statements;"

- "Assess and respond to the risk of material misstatement of the financial statements due to noncompliance" with the identified laws and regulations; and

- "Identify whether there is information indicating noncompliance with those laws and regulations have or may have occurred."

The PCAOB acknowledged that its proposal would substantially increase auditors' responsibilities and burdens, including retaining outside specialists, such as fraud and legal professionals, to conduct the required assessments. The proposed standard will likely also expose auditors to added enforcement scrutiny, particularly when illegal conduct is uncovered during, or disclosed after, an audit.

Increased demands and expectations, including data analytics

The PCAOB's proposed amendments to the auditing standards related to NOCLAR would, if adopted and approved, lead external auditors to expect more from their clients with respect to demonstrating the effectiveness of a company's fraud risk management preparedness. That will likely increase the need for CFEs and internal auditors in the context of their organizations' fraud risk management program. (See *Fraud Risk Management Guide*, Second Edition, COSO and the ACFE, tinyurl.com/y3hhrt2b.) These areas could include:

- **Compliance and investigation programs.** Companies will need to assess and strengthen their programs for compliance, investigations, issues management, complaints management, etc.; overall corporate risk programs; and "high-impact" regulatory programs. Enhancements will also be needed for the identification, sizing, communication, escalation, and overall control environment of potential noncompliance and fraud.

- **Compliance risk assessments.** Organizations will need to revise and strengthen their risk assessments for complaints, investigations, self-identified issues, monitoring and testing results for laws and regulations that may not be their current focus.

- **Regulatory change.** There'll be a need for a full inventory of applicable laws, rules and regulations, mapped to business processes and controls, and used for ongoing compliance risk assessments (including inherent and residual risk). Such laws might include the U.S. Foreign Corrupt Practices Act (FCPA), U.S. Sanctions and Trade Compliance laws, International Traffic in Arms Regulations, data privacy laws, and laws for human trafficking and forced labor, etc.
- **Controls expansion and testing.** Companies will need to expand the size and scope of ongoing controls, control mapping, control accountability and control testing to those related to compliance with laws and regulations, in line with (and potentially part of) Sarbanes-Oxley (SOX) or SOX-like standards.

Lynda Schwartz, CFE, CPA, professor of practice and director of forensic accounting and data analytics curriculum at the University of Massachusetts Amherst tells *Fraud Magazine* that the PCAOB's proposed amendments to AS 2405 incorporate approaches familiar to forensic accountants and CFEs, such as regulatory-focused risk assessments, analysis of evidence, consultation with legal and compliance professionals, and gathering public information. However, she cautions that its implementation could be challenging for small public companies and auditing firms.

"Regulators, standard-setters, auditors and forensic professionals have wrestled for decades with the question of whether and to what degree an auditor can make attestations that there's no fraud and that no laws have been broken," says Schwartz. "CFEs know there's no secret decoder ring to detect fraud and noncompliance. The task's even more challenging when there's no specific predicate to investigate."

The PCAOB's proposal is expansive and could require the financial statement audit team to identify applicable laws and regulations, make legal and financial assessments regarding potential risks, and identify and evaluate regulatory vulnerabilities long before they're resolved.

"The AS 2405 proposal may encompass regulatory exposures outside of financial statement auditors' traditional areas of expertise, such as dangerous workplaces, environmental harms, privacy and data breaches, and global regulations. As proposed, it will be a heavy lift for public companies and the auditing profession," says Schwartz.

The PCAOB has also proposed amendments to AS 1105 related to aspects of "Designing and Performing Audit Procedures That Involve Technology-Assisted Analysis of Information in Electronic Form." The amendments, expected to be adopted this year, will increase the data analytics and transaction-monitoring expectations for auditors related to testing of vendors, customers, employees and other aspects. According to PCAOB Release No. 2023-003, the proposed changes stem from the results of the PCAOB's research project on data and technology indicating that auditors are expanding their use of technology-based tools to plan and perform audits. (See "Data and Technology," PCAOB, updated Nov. 30, 2022, tinyurl.com/35rrs2px.) The PCAOB's release says that despite its research, there's a need for amendments to address designing and performing audit procedures that use technology-assisted analysis of information in electronic form. (See "Amendments Related to Aspects of Designing and Performing Audit Procedures That Involve Technology-Assisted Analysis of Information in Electronic Form," PCAOB, updated June 26, 2023, tinyurl.com/ycy44dbs.)

While there isn't a single software solution to comply with all aspects of the new PCAOB fraud rules, several analytics tools can assist companies in different areas:

- **Continuous transaction monitoring (CTM).** These systems monitor financial transactions for anomalies or control violations that might indicate fraud. Without picking samples, software platforms can now analyze billions of transactions related to vendor, customer and employee activities, applying hundreds of targeted tests and algorithms to risk rank them for relevancy — identifying unusual patterns in spending, receivables or disbursements.
- **Data visualization tools.** These can help CFEs, auditors and company personnel understand complex financial data and identify potential risks at a higher level compared to traditional spreadsheets. By presenting information visually, users can flag inconsistencies or areas requiring further

investigation and drill down into the data.

- **Text analytics.** These tools can analyze large volumes of text data, such as free text descriptions in payments, contracts or internal communications. This can help identify potential red flags like unusual language or sentiment that might indicate fraud. Nobody references "bribe expense," but they'll create codewords like "volume facilitation payment" or "help fee" to describe an improper payment.

- **Artificial intelligence (AI) and machine learning.** AI and machine learning have been around for decades. Training high-risk transactions to "find more like this" with machine learning (a subset of AI) is highly effective in identifying potentially improper payments or transactions,

and companies are increasingly adopting it for their fraud risk management programs. (See "Using technology-assisted review to uncover suspicious transactions," by Vincent Walden, CFE, CPA, *Fraud Magazine*, November/December 2022, tinyurl.com/4xu6kjph.) The current buzz is about generative AI, which taps into large language models to generate content in response to a prompt. Where it gets interesting, from a fraud-risk-management perspective, is when these large language models become domain specific about regulatory matters and company data to provide insights to the user (or the auditor). (See "Can generative AI give us prescriptive analytics?" by Vincent Walden, CFE, CPA, *Fraud*

Magazine, March/April 2024, tinyurl.com/46x4ja84.)

Remember that analytics software is a supportive tool, not a silver bullet. Companies will always need strong internal controls, competent professionals such as CFEs, a culture of ethics, and collaboration with auditors to effectively comply with new PCAOB rules. ■ **FM**

Vincent M. Walden, **CFE, CPA**, is the CEO of Kona AI, an AI-driven anti-fraud, investigations and compliance technology software company providing easy-to-use, cost-effective vendor, customer and employee transaction risk analytics. He works closely with CFEs, internal auditors, compliance, audit, legal and finance professionals and welcomes your feedback and ideas. Contact Walden at vwalden@konaai.com.