PCAOB Rule Making Docket Matter No. 051

Robert Conway Response to Request for Public Comment re

Questions Posed in the NOCLAR Roundtable Briefing Paper

March 17, 2024

About the Author – Robert Conway, CPA

I am a retired KPMG audit partner. I also spent nine years at the PCAOB leading inspections of Big Four audits. I also had leadership responsibility for the PCAOB regional offices in Los Angeles and Orange County. After the PCAOB, I served for three years as the Professional Practice Director for an 80-person regional CPA firm that exclusively consulted on technical accounting matters and Sarbanes-Oxley compliance. Over the last four years, I have served as an expert witness on several high-profile disputes in litigation involving the application of auditing and accounting standards for public companies.

My Response

I am responding to the PCAOB's request for public comment on its NOCLAR Roundtable Briefing Paper and the Roundtable Panel Discussions. My response begins with a series of overarching observations. I have also responded herein to each of the questions posed by the PCAOB in its Roundtable Briefing Paper.

I previously responded to the PCAOB's request for public comment on the originally proposed amendments to the PCAOB's Illegal Acts standard.

Overall Observations from the Roundtable

A. **What problem are we trying to solve?** This came up several times during the Roundtable discussion. I am not sure any clarity on this most basic question was achieved in either in the Roundtable Briefing Paper or the Roundtable Discussion. Step #1 is to define the problem that needs to be solved. I encourage the PCAOB to cite real-world examples of the types of problems the PCAOB is seeking to prevent or detect earlier. Some root cause analysis of what went wrong in each of those examples would facilitate identification of the responsible parties and possible solutions to prevent or enable earlier detection of the underlying problems. Some possible solutions may involve improvements to the auditing standards, but some more cost-effective solutions may reside beyond the PCAOB's jurisdiction. In short, I favor a more holistic approach rooted in the problems the PCAOB is seeking to remedy as a means to improve investor protection.

   The PCAOB acknowledges that the proposed standard was interpreted by many respondents in a manner that was not intended. I suspect that part of the misunderstanding relates to the PCAOB's principles-based focus on standard setting. Absent the use of examples or interpretive guidance, there is a heightened risk that PCAOB work product will be misunderstood. This can be particularly problematic with standards having potentially high costs of implementation. This was a significant contributing factor to the difficulty issuers experienced implementing the PCAOB's

standard on internal controls over financial reporting. Care should be taken to avoid such misunderstandings in the future.

B. **Success in competitive markets is about managing a myriad of risks. NOCLAR is just one of many risks. Risk management is first and foremost a governance function with oversight from the issuer's board of directors**. **Investors should have more information about how issuers manage their risks of NOCLAR.** Existing disclosures in SEC filings about NOCLAR risks in the "Risk Factors" section are woefully inadequate. Investors deserve to understand 1) the issuer's perception of significant NOCLAR risks, 2) how those risks are managed and monitored by the board of directors and executive management, and 3) ongoing developments and investigations regarding NOCLAR. Expanded disclosures in forms 10-K and 10-Q would automatically be covered by existing CEO and CFO certifications under SOX 302 and 906, thereby further motivating executive management to pay particular attention to the management of NOCLAR risks as opposed to feigning ignorance and lack of responsibilities when instances of non-compliance occur.

C. **Internal audit should play an important role in the monitoring and investigating possible NOCLAR risks. This is in keeping with my view that regulatory compliance is governance function.**

D. **The enforceability of executive compensation claw back arrangements is an important tool to promote better executive management of NOCLAR risks. My general understanding is that various issues have arisen with respect to the enforceability of claw back arrangements.** Lucrative executive compensation schemes can unfortunately incentivize a "win at all costs" tone-at-the-top that can exacerbate NOCLAR. The PCAOB, SEC, and investor advocate organizations should be working collectively to create enforceable mechanisms that will mitigate the temptations of overly rich incentive compensation schemes.

E. **Auditors can benefit from further emphasis in PCAOB standards on the auditor's duty to evaluate business practices and contracts for compliance with contract law.** This is an element of auditing that should not be delegated down to the least experienced members of the audit team. Rather, it should be the explicit responsibility of the audit partner and audit manager to address legal compliance in both explicit and implied contracts. The enforceability of contracts is part of the existing revenue recognition standard. The need for auditors to focus on contract enforceability should be a point of emphasis in the PCAOB's auditing standards and inspection activities.

   In many cases, the auditor's knowledge of contract law should be sufficient to carry out the responsibilities described above. However, the auditor should be alert to situations that may warrant interpretation from legal counsel. Elements that should be addressed in the illegal acts standards should include 1) whether it is sufficient to rely on input from in-house counsel rather than external counsel and 2) whether it is acceptable to rely on discussions with counsel in lieu of a written communication.

F. **An alternative for assuring better auditor awareness of NOCLAR (at least on par with the issuer's knowledge):** The external auditor receives information about NOCLAR from the issuer through a narrow funnel that may be limited to the CEO and CFO (largely through management representation letters), and letters from legal counsel. As it pertains to the CEO and CFO, there is always the risk of management override that may keep the auditors in the dark. As it pertains to communications from counsel, we know that such communications tend to be limited, cryptic, and buried in disclaimers and qualifying language. In my original public comment letter (attached), I described how that funnel should be broadened by leveraging on the cascading certifications that most companies use to support the CEO and CFO officer certification under SOX sections 302 and 906. My suggestion was that steps be taken to assure that sub-certifications are obtained from each of the issuer's employees responsible for protecting the issuer from NOCLAR in their respective areas. Ideally, the sub-certifications from such individuals should be tailored to answer basic questions such as:

   a. Identify the existence of any investigations conducted by regulatory organizations or government agencies or the issuer that were completed during the last 15 months or are on-going as of the date of this certification.
   b. Identify all communications between the issuer and such organizations during the last 15 months.
   c. Understand each employee's current perspective on regulatory compliance and whether there any areas of concern.

   Sub-certifications from Internal Audit should be similarly tailored to assure that their awareness of possible NOCLAR events rises to the auditor's attention.

G. **We can all agree that the auditor should have visibility to the issuer's risk assessment for NOCLAR and the issuer's related processes and controls. Beyond that, I see the following possibilities for auditor involvement (at both ends of a wide spectrum):**

   a. Assure that the auditor has visibility to existing events of NOCLAR at year-end that is at least comparable to the issuer's existing knowledge.
   b. Identify all events of possible NOCLAR with potentially material impact to current or future financial statements (**including those which the issuer may not currently be aware of**).

   There is an enormous difference in cost between scenarios "a" and "b." I believe the PCAOB said that it did not intend the extensive and costly approach that many commenters (including me) expressed concern about (scenario "b").

   However, if the PCAOB plans to pursue scenario "b", the PCAOB needs to quantify the cost of scenario "b" and the uncertainty of achieving the desired benefits.

H. **Audits have historically identified only 4% of fraud.** The Association of Certified Fraud Examiners (ACFE) periodically produces a report on the nature of occupational fraud[1] and how it may be identified. The data contained in ACFE's *Occupational Fraud 2022: A Report to the Nations* "represents our [ACFE's] best effort to understand and measure the impact of occupation fraud. Based on 2,110 cases of occupational fraud that were under investigation between January 2020 and September 2021, we have compiled statistics on the methods used to commit these crimes, … [how] they were detected, the characteristics of both the victims and the perpetrators, … ."[2] The ACFE's 2022 study, indicated that audits identified fraud in only 4% of the 2,110 cases of fraud studied. Several other sources that were more prolific identifiers of fraud included tips (42%), internal audit (16%), management review (12%), document examination (6%), by accident (5%), account reconciliation (5%), and automated transaction/data monitoring (4%).

   Furthermore, we know that auditor reporting on internal controls over financial reporting has been a lagging indicator of restatements rather than a leading indicator of restatements. We also know from PCAOB inspection results that the largest audit firms are struggling to comply with existing standards.

   The above information calls into question whether complex auditor-dependent solutions to mitigate NOCLAR risks will be successful and cost-effective.

I. **In January 2024, The Committee on Sponsoring Organizations (COSO) issued a request for proposals seeking assistance with the development of a Corporate Governance Framework.** It is my hope and expectation that a COSO Corporate Governance Framework will create a high degree of accountability for issuer board and executive management of NOCLAR risk. I would also expect clarification as to the auditor's role and degree of involvement in corporate governance with respect to NOCLAR. The PCAOB should obviously monitor the progress of the COSO Governance Framework project for the role auditors should play in NOCLAR risk management and detection.

In many instances, the above observations are described further in my responses to the PCAOB questions posed in the PCAOB's Roundtable Briefing Paper.

---

[1] Occupational fraud is formally defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

[2] See page 22 at 2022+Report+to+the+Nations.pdf (amazonaws.com)

Robert Conway Responses to Questions

Posed in the

PCAOB's NOCLAR Briefing Paper

PANEL I: IDENTIFICATION

Topic (1): Threshold for Identification of Laws and Regulations

Questions Related to this Topic:

1. Are there other thresholds besides "could reasonably have a material effect" that would provide sufficient rigor to the auditors' identification of laws and regulations relevant to the audit of a company's financial statements?

This received a good degree of discussion during the Roundtable. The discussion seemed to favor "likely possible" (a higher standard) over a lower standard of "more likely than not." I would favor the higher threshold over a lower threshold.

2. What types of specific procedures should the auditor perform to identify the laws and regulations? Are any of these procedures already required, at least in part, by Section 10A of the Exchange Act or procedures required by existing PCAOB standards? Should auditors be able to consider the work of management in identifying laws and regulations and if so, how?

A logical place to start would be management's risk assessment program and the risks that management believes warrant programs to prevent NOCLAR. I would expect that all public companies should have a risk assessment program that speaks to the risk of NOCLAR along with the titles of personnel responsible for assuring compliance and interacting with regulators and law enforcement. If there is no such requirement to have a formalized program of this nature, then such a requirement should be required.

If such programs are not currently required, I would expect that programs to manage NOCLAR risk would be an outcome of COSO's work on a governance framework.

Anything mentioned in the Risk Factor sections of periodic filings should also be considered during the auditor's assessment of NOCLAR risk.

Past areas that have led to fines or sanctions should also be considered.

I am surprised that programs to prevent NOCLAR are not required subject matter in Form 10-K. If such a requirement existed, the CEO and CFO SOX 302 and 906 certifications as currently formulated would motivate executive management to be sure appropriate resources were devoted to preventing NOCLAR.

3. What potential approaches in the standard would facilitate auditors in identifying such laws and regulations (e.g., factors to determine the relevant population of laws and regulations; factors that relate to the risk of material misstatement due to noncompliance with laws and regulations)?

See above.

Topic (2): Direct Illegal Acts vs. Indirect Illegal Acts

Questions Related to this Topic:

1. Given that noncompliance with both direct and indirect laws and regulations can result in material misstatements of the financial statements, what is your view of the direct/indirect distinction under the current PCAOB auditing standard?

I have not found the distinction between direct and indirect to be confusing. Any confusion among investors could be reduced by explaining the distinction in the auditor's opinion.

2. How are auditors and management assessing violations of an indirect law or regulation that results in a contingent liability that when not correctly recorded or disclosed misstates the financial statements? Does the direct or indirect nature of the law violated matter to this assessment?

Matters in the Indirect Category

When indirect matters come to the attention of auditors, my experience has been that auditors are good about communicating to the audit committee and seeing that such matters are appropriately investigated by the issuer (in most cases by independent external counsel hired by the audit committee).

I believe the current interest in improving the audit standards with respect to NOCLAR pertain to the following instances in the indirect category:

a. Instances in the indirect category where the issuer may be in NOCLAR, but is not aware of such non-compliance,
b. Instances in the indirect category where someone in the issuer organization is aware of possible NOCLAR, but such matters have not been communicated to the issuer's Disclosure Committee.
c. Instances in the indirect category where executive management is aware of possible NOCLAR, but the auditor has not been made aware of such matters.

The sticky wicket is category "a" above. This is the area where auditor procedures to identify such instances of NOCLAR may be prohibitively costly. I say "may be prohibitively costly" because the PCAOB has not scratched the surface on whether the cost-benefit relationship favors incremental effort by auditors. I described an approach for the PCAOB to conduct such a study in my original public comment on the proposed NOCLAR standard; however, it seems that no such study has been conducted. Instead, I heard the PCAOB make a general request to see if anyone might come forward with supporting information. My personal view is that considering the potential enormity of the cost of such audit work, I would have expected a cost-benefit analysis would have been a prerequisite to proposing the NOCLAR standard.

With respect to items "b" and "c" above, I believe there are various opportunities to leverage off of the issuers' sub-certification processes, with particular attention devoted to tailoring the form and nature of sub-certifications from those within the issuer organization specifically tasked with ensuring and/or monitoring compliance in each specific area of laws and regulations that are relevant to each issuer (at locations/operations in domestic and international jurisdictions). As it stands currently, I believe there may be diversity in practice

across audit firms and audit teams in terms of auditor scrutiny of the sub-certifications and the form and content of such sub-certifications. I spoke to this in my original public comment. I received input from various interested parties that my original recommendation was both reasonable and actionable.

I would also take a look at auditor procedures around the issuer's disclosure committee. This is another area where there may be diversity in auditor practice. Further scrutiny in this area may reveal "better practices" that should be incorporated into audit standard revisions.

I also believe there may be diversity in practice with respect to the auditor's scrutiny of information coming through the issuer whistleblowing channels. A high degree of scrutiny and more uniform analysis of the disposition of such communications may serve to better alert the auditor to matters possibly indicative of NOCLAR that may not have received appropriate attention from management. This too was in my original public comment.

The Direct Category

Matters in the "direct" category are more generally within the auditor's skill set and may be resolved without substantial assistance from outside the audit team. In some instances, however, auditor conclusions on an accounting matter may depend on legal interpretations of contractual matters. The PCAOB should give some consideration as to whether it is sufficient for audit teams to rely on interpretations from in-house counsel (bearing in mind that in-house counsel is expected to be a zealous advocate for the client and that AS 2505.08 provides that "evidential matter obtained from inside counsel is not a substitute for information outside counsel refuses to furnish."). The PCAOB may also want to address whether the communications from counsel should be in writing.

PANEL II: CONSIDERATIONS FOR AN AUDITOR'S ASSESSMENT OF NONCOMPLIANCE AND OTHER LEGAL CONSIDERATIONS

Topic (1): Competence to assess relevant noncompliance with laws and regulations

Questions Related to this Topic:

1. How are auditors currently complying with the existing requirements of Section 10A(b)(1)(A)(i) which requires auditors to determine whether it is likely that an illegal act has occurred, when the firm detects or otherwise becomes aware of information indicating that an illegal act has or may have occurred?

When matters in the "indirect" category of possible illegal acts come to the attention of auditors, my experience has been that auditors are good about communicating to the audit committee and seeing that such matters are appropriately investigated by the issuer (in most cases by independent external counsel hired by the audit committee).

I do not believe PCAOB standards require the engagement team to communicate with the audit firm's national office when a potential illegal act comes to the auditor's attention. I believe the PCAOB should mandate such communications to the national office as an additional safeguard to prevent the engagement team from "looking the other way" to avoid jeopardizing the audit client relationship. The possibility of this becoming a problem increases with the size of the audit fee. If an auditor has the backing of the national office, the auditor is more likely to follow through and "do the right thing."

2. When an auditor detects or otherwise becomes aware that an illegal act may have occurred, does the evaluation of a potential illegal act differ with respect to direct and indirect laws and regulations? What are those differences in the evaluation process?

In most instances when the auditor becomes aware of a "**direct**" possible illegal act, the audit firm is typically able to resolve such matters using resources from within the audit firm. Matters in the "direct" category are likely to involve matters concerning the application of accounting standards in familiar areas such income taxes, pensions, and contracts with customers and vendors.

With respect to possible illegal acts in the "**indirect**" category, my experience has been that such matters require an independent investigation that often leads to the audit committee engaging external independent counsel.

3. When an auditor has identified or otherwise becomes aware of a potential illegal act, what is the interaction between the auditor and those hired or employed by the company to perform an investigation? For example, do auditors evaluate the work performed by such personnel as part of performing their assessment? If so, what does such an evaluation entail? Do auditors have input into how the investigation is conducted for purposes of its sufficiency for the audit? Do auditors receive debriefings on interviews of key witnesses in such investigations?

When possible illegal acts come to the attention of auditors, my experience has been that auditors are good about communicating to the audit committee and seeing that such matters are appropriately investigated by the issuer (in most cases by independent external counsel hired by the audit committee). My experience has been that the commonality of interest between the attorney and the auditor favors regular oral updates by the attorney to the auditor and audit committee. Auditor discussions with the audit committee help to ensure that the auditor has briefings and conclusions reached by external counsel that are sufficient for the auditor's purposes. A letter of audit inquiry to the external counsel is also an avenue to assure that the auditor has the understanding they need to assure that the issuer's financial reporting and disclosures are sufficient.

4. What specific auditing procedures can auditors perform to identify and assess either (1) laws and regulations with which noncompliance could reasonably have a material effect on a company's financial statements or (2) the related assessment of the risk of material misstatement that are within the auditor's skillset (e.g., reading relevant minutes, inquiring of compliance personnel, examining whistleblower hotline records, reading regulatory correspondence)?

Please refer to my response to Panel 1, Topic (2), question 2 re the issuer's sub-certification process, the Disclosure Committee activity, and 3) the whistleblower in-take process.

Topic (2): Concerns Regarding Potential Waiver of Attorney-Client Privilege

Questions Related to this Topic:

1. In light of the attorney-client privilege issues raised by some commenters, how do audit firms currently comply with requirements of PCAOB standards and Section 10A of the Exchange Act?

See my answer to Panel 2, Topic (1), question 3 (above). In my 17 years as an audit partner and in my four years as an expert witness, I have seen audit committees bring about

corrective remedial action such that communications to the SEC have not been necessary. This excludes auditor communications that become necessary when there is a disagreement over accounting matters that resulted in an auditor change.

2. How would the proposed amendments affect the privilege differently than current audit requirements?

I cannot respond as I do not have the necessary legal knowledge about privilege.

3. Commenters and staff have observed that noncompliance with laws and regulations are typically identified by issuers through means (which are nonprivileged) such as, systems designed to address violations of laws and regulations or company policy (e.g., ethics and compliance hotline). Are there other common areas of identification of noncompliance such as through privileged communications? Where privileged communications are the source for a company's knowledge of noncompliance, in what situations do companies disclose the noncompliance to third parties including auditors, investors, regulators, and/or criminal authorities?

The executives at most companies are focused on "doing the right thing" and regularly confer with internal or external counsel and the audit committee to be sure they take appropriate action and make disclosures when appropriate. The Disclosure Committee processes are a good example where, under ideal circumstances, issues come to the attention of executive management and counsel. Cyber-attacks and white collar crime are examples that come to mind. Internal auditors may also be a source for the identification of issues that get communicated to executive management. In some cases, such events may be required to be communicated in a timely manner to the audit committee, relevant regulatory bodies, and law enforcement.

4. In addition to commenters' concerns regarding the potential waiver of attorney-client privilege, how do the considerations above relate to the potential waiver of work-product protection? Do the proposed amendments affect work product differently?

No comment because attorney-client privilege is beyond my area of expertise.

PANEL III: ECONOMIC IMPACTS

Questions Related to this Topic:

1. What do panelists or commenters perceive as the economic benefits and costs of the proposal and how do they differ from the status quo, both quantitatively and qualitatively? Whenever possible, provide your responses separately by firm size (e.g., large, medium, small) and stakeholder (e.g., preparers).

As I have commented earlier, there is potentially a large cost with an uncertain benefit. More work needs to be done to evaluate the cost-benefit relationship before proceeding further.

2. Please share any additional data or studies to clarify the economic impacts. Are panelists or commenters aware of additional data or studies on the current cost of unidentified noncompliance with laws and regulations on investors?

My response to the original proposal described a methodology for the PCAOB to estimate the potential cost and the potential benefit.

3. What do panelists or commenters perceive as the impact of the proposal on small- and medium sized audit firms and how have you quantified such impact?

No basis to comment.

4. What broader impacts have you determined of auditors' identification of noncompliance with laws and regulations that could reasonably have a material effect on the financial statements to the capital formation or, more broadly, macro socioeconomic environment? Are there data or studies that can help us estimate those impacts? For instance, is there evidence to suggest that capital costs would be lower if investors had greater confidence that auditors would identify noncompliance with laws and regulations that could reasonably have a material effect on the financial statements?

See my response to item "H" on page 3 of this paper.

5. To the extent panelists or commenters provide additional alternatives, are there data or studies that can help us estimate the benefits and costs of any of these alternatives?

I am surprised that the PCAOB did not make an attempt to quantify the cost impact of its proposal. My original response to the proposed standard included a methodology for estimating the cost and potential benefit.

6. In light of the discussion of costs and benefits, how do investors, issuers, and auditors view the justification of the proposal?

I cannot answer this question without a suitable analysis of the costs and potential benefit. We should remember that during the early stages of the rollout of the SOX 404 re ICFR, the SEC floated an estimate of implementation costs of less than $100,000 which was a painfully inaccurate estimate. Appropriate care should be taken to assure that mistake is not repeated.

In discussing these costs and benefits, **we strongly encourage panelists to be prepared to discuss the quantitative impact of the proposal on audit fees**; issuers' internal costs as a result of identification, evaluation, and communication of information indicating that noncompliance with laws and regulations has or may have occurred; auditors' existing reliance on compliance work and legal analyses already carried out by issuers; and potential costs associated with auditor's use of specialists.

I am surprised that the PCAOB did not make any attempt to quantify the cost of its proposal. My original response to the proposed standard included a methodology for estimating the cost and potential benefit.