March 12, 2024

Via e-mail to comments@pcaobus.org

Public Company Accounting Oversight Board
Attn: Office of the Secretary
1666 K Street N.W.
Washington, DC 20006-2803

RE: Docket 051: Amendments to PCAOB Auditing Standards related to a Company's Noncompliance with Laws and Regulation

Dear PCAOB:

As a follow-up to our comment letter dated August 1, 2023, and in light of the March 6, 2024 Virtual Roundtable on the NOCLAR Proposal of June 2023, I am writing on behalf of the Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA), a 19,000-member organization comprised of Compliance & Ethics Professionals and dedicated to serving the compliance profession globally, including many of us who have backgrounds in auditing.

Thank you so much for hosting the Virtual Roundtable, which was very helpful in so many ways. This comment letter focuses on an important issue that emerged during the virtual roundtable.

The auditors involved in the roundtable clearly were more concerned with how the proposed standards address the risk of undetected noncompliance than they are with proposed changes involving procedures and discussions with management around known/detected noncompliance. Their concern seems to lie at the heart of the recommendations we made in our August comment letter, which I would like to expand upon and clarify here as part of a two-part recommendation.

Analysis

Proposed AS 2110.26 requires that auditors gain an understanding of various management processes, including the process for, among other things (note that items a, b, and c are omitted here since they are not relevant to this discussion):

d. "Identifying laws and regulations with which noncompliance could reasonably have a material effect on the financial statements;

e. Preventing, identifying, investigating, evaluating, communicating (including to senior management, the audit committee, and the board of directors), and remediating instances, or alleged or suspected instances, of fraud or other noncompliance with laws and regulations" and for
f. "Receiving and responding to tips and complaints from internal and external parties regarding instances, or alleged or suspected instances, of fraud or other noncompliance with laws and regulations (including those received through a whistleblower program, if such program exists)"

AS 2110.26d, e, and f represent several of the key elements of a compliance and ethics program, the aim of which is the prevention, detection, investigation, and remediation of noncompliance (see United States Sentencing Commission Sentencing Guidelines, Chapter 8, Sentencing of Organizations, §8B2.1(a) and (b)(1)-(7) and (c) under "Effective Compliance and Ethics Program"). https://www.ussc.gov/guidelines/2023-guidelines-manual/annotated-2023-chapter-8

Proposed AS 2110.54 and .56 are the two primary, relevant sections devoted to inquiries auditors should make in connection with gaining this understanding. However, both of these sections focus on the identification of known instances of noncompliance through the auditor's inquiries, rather than the broader understanding of the compliance program as described in AS 2110.26, such as the identification and assessment of compliance risks, and the design and implementation of preventive and detective measures, which would typically include:

- Compliance-related policies and procedures
- Compliance training
- Compliance auditing and monitoring
- Compliance-related communications in support of the compliance and ethics program
- The processes involved in receiving reports of alleged noncompliance (not just whether allegations have been received through a hotline, but the entire process itself)

For example, the note to AS 2110.54, which requires inquiries of the audit committee or its equivalent, states that such inquiry should address known, alleged, or suspected instances of noncompliance. It does not require inquiry about the preventive or detective measures.

Similarly, AS 2110.56, which requires inquiries of management, the audit committee, and the internal audit function, focuses most of those inquiries on "instances, or alleged or suspected instances" of noncompliance. The closest that AS 2110.56 gets to inquiries about the design and operation of preventive and detective measures of the compliance program is in 2110.56(a)(3), which addresses management's processes for conducting a fraud risk assessment (but fails to address a compliance risk assessment), and 2110.56(a)(4) which addresses preventive and detective controls over compliance.

Other relevant factors to consider in providing direction to auditors in making inquiries include:

- The design and operation of a compliance and ethics program is generally the responsibility of the chief compliance officer (CCO) or equivalent title; Accordingly, the person most familiar with the identification and assessment of compliance risks, and the risk mitigation efforts aimed at preventing and detecting noncompliance, is the person who is the CCO

- The CCO is often not considered "management" as that term is defined and interpreted by auditors
- Organization charts sometimes reflect the CCO reporting to general counsel, but often the reporting line is to the Chief Executive Officer, Chief Operating Officer or some other executive team member; Professional best practices and Department of Justice guidance suggests a separation between CCO and General Counsel, but in practice a wide variety of reporting structures exist
    - See U.S. Department of Justice, Criminal Division, "Evaluation of Corporate Compliance Programs" (Updated March 2023), see Part II, Section B "Autonomy and Resources", under "Structure" and "Seniority and Stature" pages 10-11 https://www.justice.gov/criminal/criminal-fraud/compliance
- Much like with an internal audit function, some companies, particularly smaller ones, may not have a distinct compliance function; While this is not a recommended practice, it is a fact that is reflected in the wording chosen for our recommendations below.

Nowhere in the proposed standards are auditors directed to make any communications with compliance personnel, even though compliance personnel are responsible for the design and implementation of the compliance and ethics program, and are often the first to hear of allegations of noncompliance through the hotline system.

Recommendations

To address these issues, resulting in improved and clarified guidance for auditors, we recommend the following changes to the proposed standards:

1. Require in AS 2110.56 that auditors make inquiries about a company's process for identifying and assessing compliance risks (to provide the "how to" follow-up to AS 2110.26d, e, and f, which require that auditors "obtain an understanding")
2. Related to the preceding recommendation, add a new section, AS 2110.56d stating "If the company has a compliance function, inquiries of appropriate compliance personnel regarding the processes used for the identification and assessment of laws and regulations that could reasonably have a material effect of the financial statements, and the prevention, detection, investigation, and remediation of noncompliance" (to close the gap that exists in the proposed language that relies solely on inquiries of management, audit committees, and internal auditors to gain this understanding)

Summary and Closing

Thank you very much for the PCAOB's efforts to modernize this area of the auditing standards and for the opportunity to submit these comments.

Sincerely,

Gerard M. Zack, Chief Executive Officer
Society of Corporate Compliance & Health Care Compliance Association
6462 City West Parkway
Eden Prairie, MN 55344
Tel: +1 952.567.6215
E-mail: Gerry.Zack@corporatecompliance.org

APPENDIX – Relevant Sections from SCCE & HCCA's August 1, 2023 Comment Letter

Background and Organizational Positioning of Compliance

For more than 30 years Chapter 8, Part B2 (titled "Effective Compliance and Ethics Program") of the United States Sentencing Commission's Organizational Sentencing Guidelines has served as the standard for programs designed to prevent and detect non-compliance with laws, particularly criminal laws which are most likely to lead to adverse consequences for public companies. In 2004, the United States Sentencing Commission revised and strengthened Chapter 8B2 of the Guidelines in response to a directive contained in the Sarbanes-Oxley Act to ensure that "the guidelines that apply to organizations… are sufficient to deter and punish organizational criminal misconduct." Chapter 8B2 has long been recognized as the framework around which effective programs to prevent and detect non-compliance with laws and regulations should be constructed. Other Federal Agencies have built on these standards.

For example, in 1998 the U.S. Department of Health and Human Services, Office of Inspector General, published its **Compliance Program Guidance for Hospitals**. This guidance provides some of the earliest support for what has become a best practice today of segregating the compliance function from that of internal legal counsel, noting that "Designating a compliance officer with the appropriate authority is critical to the success of the program, necessitating the appointment of a high-level official in the hospital with direct access to the hospital's governing body and the CEO." A footnote to this sentence states "The OIG believes that there is some risk to establishing an independent compliance function if that function is subordinance [*sic*] to the hospital's general counsel, or comptroller or similar hospital financial officer. Free standing compliance functions help to ensure independent and objective legal reviews and financial analyses of the institution's compliance efforts and activities. By separating the compliance function from the key management positions of general counsel or chief hospital financial officer (where the size and structure of the hospital make this a feasible option), a system of checks and balances is established to more effectively achieve the goals of the compliance program."

If we fast-forward 25 years, the U.S. Department of Justice (DoJ), Criminal Division, **Evaluation of Corporate Compliance Programs** (Updated March 2023) includes the following expectation in section B (Autonomy and Resources): "(3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee". The DoJ guidance expands on this by asking the structural question: "Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)?"

Moreover, during the past few decades, numerous deferred prosecution agreements, Corporate Integrity Agreements and other settlements by corporate wrongdoers have incorporated the Chapter 8B2 framework and numerous judicial decisions have held to account organizations which failed to adhere to the framework.

Clearly, a best practice has emerged in which the compliance function is segregated from internal legal counsel and other management functions or, at a minimum, it operates in a manner similar to how the

internal audit function normally operates, where it may report to a member of management on a daily basis, but has direct access and reports to the audit committee (or its equivalent) without other members of management present.

Auditing Standards Should Explicitly Require Inquiries of Compliance Personnel

Proposed auditing standard 2405.06a requires that auditors perform certain compliance-related risk assessment procedures in connection with planning the audit, including:

1) "Obtaining an understanding of the company and its environment, including the regulatory environment (see paragraphs .07-.15 of AS 2110, Identifying and Assessing Risks of Material Misstatement [as proposed to be amended]);
2) Obtaining an understanding of management's processes related to (i) identifying laws and regulations with which noncompliance could reasonably have a material effect on the financial statements; (ii) preventing, identifying, investigating, evaluating, communicating, and remediating instances of noncompliance with laws and regulations; (iii) receiving and responding to tips and complaints from internal and external parties regarding noncompliance with laws and regulations; and (iv) evaluating potential accounting and disclosure implications of noncompliance with laws and regulations, including fraud (see AS 2110.26 [as proposed to be amended]);
3) Making inquiries of management, the audit committee, internal audit personnel, and others regarding noncompliance with laws and regulations (see AS 2110.54 and .56-.58 [as proposed to be amended])"

Additional guidance is provided in the proposed changes to AS 2110, the broader standard on identifying and assessing risks of misstatement (whether related to noncompliance, fraud, or any other reason), which includes several proposed changes that we feel should be modified.

Proposed AS 2110.26 requires that auditors gain an understanding of various management processes, including the process for:

d) "preventing, identifying, investigating, evaluating, communicating (including to senior management, the audit committee, and the board of directors), and remediating instances, or alleged or suspected instances, of fraud or other noncompliance with laws and regulations" and for
e) "receiving and responding to tips and complaints from internal and external parties regarding instances, or alleged or suspected instances, of fraud or other noncompliance with laws and regulations (including those received through a whistleblower program, if such program exists)"

Proposed changes to AS 2110.56 and .57 address the inquiries that auditors should make in connection with understanding whether an auditee is aware of instances of fraud or noncompliance. These inquiries include those with management (AS 2110.56a), the audit committee (AS 2110.56b), the internal audit function, if one exists (AS 2110.56c), and "others within the company" (AS 2110.57). Included among "others" is in-house legal counsel (AS 2110.57d).

Our concern lies in the fact that AS 2110 and 2405 require auditors to gain an understanding of compliance risks and several key elements of the compliance and ethics program by performing various procedures, including having communications with auditee personnel. **However, the proposed standards fail to require any communication with the person(s) that have the greatest knowledge of compliance risk, compliance risk assessments, the hotline, and the overall compliance program – the head of the compliance function and other key compliance leaders.**

Learning about compliance risks and how a company manages those risks by communicating with senior management, the audit committee, and potentially internal general counsel deprives auditors of the best source of information regarding compliance risks.

As noted by the PCAOB in its "Discussion of Proposal" section of the proposal, many auditors do consult with the head of compliance. Clearly, this has emerged as a best practice and should be specifically required.

We feel strongly that communication with the Chief Compliance Officer (or equivalent title in charge of the compliance function) is absolutely essential to accomplishing what PCAOB is aiming for with these proposed changes, and it should be explicitly stated so in at least the following two places:

- **AS 2405.06a3**
- **AS 2110.56 (it should be added as new AS 2110.56d)**

The vast majority of public companies have a compliance function. And as noted earlier, best practice of segregating compliance from internal legal counsel is strongly preferred and now also appears to be the case with the majority of large companies. To accommodate those few companies that do not have a compliance function, PCAOB could consider using language similar to what it uses in AS 2110.56c, where a requirement begins with "If the company has an internal audit function,…..". Similar language could be used with respect to this inquiry of the chief compliance officer (e.g. "If the company has a compliance function…").

Board or Audit Committee Oversight of the Compliance Program

On a related matter, the proposed standard's guidance on inquiries of the audit committee (See AS 2110.56b(5)) states that auditors should ask about how the committee exercises oversight of the fraud risk assessment process, but it does not ask about compliance risk oversight.

As noted earlier, in 1991, Chapter 8, Sentencing of Organizations, of the United States Sentencing Guidelines (USSG), from the U.S. Sentencing Commission, established much of what is today considered the framework of compliance and ethics programs. USSG §8B2.1(b)(2)(A) requires that "the organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program."

In connection with this responsibility, the previously referenced guidance from U.S. Department of Justice (DoJ), Criminal Division, **Evaluation of Corporate Compliance Programs** (Updated March 2023) asks the following questions in connection with evaluating a company's compliance and ethics program in a section II. "Is the Corporation's Compliance program Adequately Resourced and Empowered to Function Effectively?" Subpart A on "Commitment by Senior and Middle Management":

- Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions?
- What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

This guidance has become widely accepted and audit committees (or some similar board-level committee) is expected to provide oversight of the compliance and ethics program, including the compliance risk assessment process utilized by the compliance function.

Additionally, it is important to note that a company's internally-prepared fraud risk assessment is normally prepared by different individuals than those who prepare the compliance risk assessment. The compliance risk assessment is normally prepared by the compliance function, whereas the fraud risk assessment is often prepared by a finance or other function. And while communication between individuals involved in the fraud risk assessment and the compliance risk assessment is a valuable practice, it should not be assumed to occur in all companies.

Accordingly, we suggest that proposed AS 2110.56b(5), addressing inquiries of the audit committee, be modified as follows (suggested changes underlined):

How the audit committee exercises oversight of the company's assessment of fraud risk <u>and the risk of noncompliance</u> and the establishment of controls to address fraud risks or that otherwise help to prevent and detect fraud or other noncompliance with laws and regulations that could reasonably have a material effect on the financial statements;

<u>Supplemental PCAOB Staff Guidance – Reference to Chapter 8B2</u>

Chapter 8B2 of the Sentencing Guidelines, referenced in connection with our previous comments in this letter, has become the gold standard for compliance and ethics programs. The Chapter 8B2 expectations of an effective compliance and ethics program are specifically referenced in guidance from several U.S. government agencies, including the Department of Justice, Department of Health and Human Services, Securities and Exchange Commission, and Environmental Protection Agency. Other agencies have patterned guidance after Chapter 8B2 without explicit references.

If auditors are expected to gain an understanding of how management identifies and manages compliance risk as part of assessing the risk of material misstatement resulting from noncompliance (proposed AS 2110.26d, e and f), understanding whether the compliance and ethics program implemented by the company meets the standards established by Chapter 8B2 would provide extremely valuable insight to the auditors. While auditors are certainly not expected to reach a conclusion

regarding, or opine on, the effectiveness of a compliance and ethics program, understanding the characteristics of an effective program would greatly help auditors in making determinations regarding the risk of material misstatement resulting from noncompliance.

Making reference to Chapter 8B2 directly in the auditing standards would accomplish this, but may be inconsistent with PCAOB's approach to addressing such issues. Rather, PCAOB often provides supplemental guidance on implementation of auditing standards.

Accordingly, we urge PCAOB to publish supplemental guidance to auditors that includes the establishment of Chapter 8B2 as the standard by which auditors should consider the effectiveness of a company's compliance and ethics program in connection with assessing the risk of material misstatement.