PCAOB
PUBLIC COMPANY ACCOUNTING
OVERSIGHT BOARD

June 6, 2024

<u>By Electronic Mail</u>
The Honorable Gary Gensler
The Honorable Hester M. Peirce
The Honorable Caroline A. Crenshaw
The Honorable Mark T. Uyeda
The Honorable Jaime Lizárraga
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chair Gensler and Commissioners Peirce, Crenshaw, Uyeda, and Lizárraga:

I am pleased to transmit to you a summary of the Public Company Accounting Oversight Board (PCAOB or Board) Office of Internal Oversight and Performance Assurance's (IOPA) Program Review Report: *Office of Enterprise Risk Management* (June 2024). The Board formed IOPA to promote the confidence of Congress, the Securities and Exchange Commission, and the public in the integrity of PCAOB programs and operations. IOPA conducted this review in conformance with the Institute of Internal Auditors' (The IIA) *International Standards for the Professional Practice of Internal Auditing*.

IOPA undertook this review to evaluate the efficacy of the Office of Enterprise Risk Management's (OERM or the Office) internal controls and processes, which IOPA tested for adequate design and effectiveness. This was the first time IOPA has performed a comprehensive review of the OERM function, which was created in furtherance of the PCAOB's 2018 – 2022 Strategic Plan. In February 2019, the PCAOB hired its first Chief Risk Officer to head the newly created office, and the Ethics and Compliance Program (Ethics) moved from the PCAOB's Office of the General Counsel to OERM.

As the summary report sets forth, IOPA found that, in a relatively short five-year period, OERM has done a commendable job in creating and growing a sophisticated second line enterprise risk management function, consistent with The IIA's *Three Lines Model*, which promotes structured communication and collaboration between an organization's first line (operating management), second line (specialists assisting first line with managing risk), and third line (independent internal audit function). Generally, OERM has created well-documented guidance and procedures, as well as a comprehensive organizational risk register and detailed risk reporting. The Office has established strong lines of communication and frequent engagement with PCAOB Divisions and Offices (D/Os). Additionally, OERM has been recognized throughout the organization for its crucial work and leadership responding to COVID-19, which was both essential and effective in supporting the PCAOB during an unprecedented period. In interviewing a variety of OERM's collaborators during review fieldwork, IOPA generally found respect for and appreciation of OERM's function and activities throughout the organization.

During the review, IOPA identified certain enhancement opportunities that will enable OERM to continue ably supporting the organization. *First*, with sustained support and visibility from organizational leadership, OERM should: (a) further define and communicate the differences between first line and second line roles and responsibilities; (b) continue to look for opportunities to provide supplemental expertise and credible challenge to the PCAOB's first line; and (c) provide greater awareness to the organization of these enhancements and others incorporated by OERM to date. *Second*, in the unique and limited circumstance where OERM/Ethics is the first line function under IOPA review, the Office should complete its first line remedial efforts and then notify IOPA of the status, after which IOPA will conduct a third line review of the remedial activities. In light of the structural overlap and the importance of an objective assessment, OERM's second line tracking reports should not inform the Board and D/Os of the reasonableness of the Office's own remedial activity prior to IOPA's review and agreement.

The Board has reviewed IOPA's recommendations and management's responses thereto and has approved the transmittal of the summary report to you.

The PCAOB intends to publish the attached summary on its website on or about June 14, 2024. Please feel free to contact Michael Weigand, Director of IOPA, at (202) 591-4659 or me if you have any questions or would like any additional information about the review.

Sincerely,

Erica Y. Williams

Erica Williams
Chair

Enclosure: IOPA's Program Review Report: *Office of Enterprise Risk Management* (June 2024)

Office of Internal Oversight and Performance Assurance

Program Review: *Office of Enterprise Risk Management*
Summary Report (June 2024)

1. Executive Summary

As detailed herein, from May 2023 through March 2024, the Public Company Accounting Oversight Board's (PCAOB or "Board") Office of Internal Oversight and Performance Assurance (IOPA) conducted a program review ("Review") of the PCAOB's Office of Enterprise Risk Management (OERM or the "Office").

1.1 Review Objective and Scope

Objective: IOPA applied a range of procedures to assess the efficacy of OERM's internal controls and processes, which IOPA tested for adequate design and effectiveness. Based on the assessment detailed herein, IOPA is recommending certain improvement opportunities for OERM.

Scope: The scope of IOPA's Review included:

- Performing process walkthroughs and evaluating documented policies and procedures for OERM's systems and processes, including OERM's Enterprise Risk Management (ERM) program (inclusive of risk assessments, risk monitoring, and risk reporting), Business Continuity Program (BCP), and Ethics and Compliance Program (ECP or "Ethics");
- Conducting interviews of:
    a. OERM leadership, to gain an understanding of work streams, initiatives, and related interactions with PCAOB Divisions and Offices (D/Os);
    b. select Board Members and Board staff; and
    c. leadership and staff in the Office of the General Counsel (OGC), Division of Registration and Inspections (DRI), Division of Enforcement and Investigations, Office of the Chief Operating Officer (including but not limited to the Office of Data, Security, and Technology (ODST)), Office of the Chief Auditor, Office of Economic and Risk Analysis, and Office of International Affairs, to understand how these D/Os collaborate with OERM staff and the effectiveness of these collaborations;
- Gathering leading ERM practice information from a prominent consulting company;
- Conducting a survey of OERM staff to gather feedback on the maturity, effectiveness, and efficiency of OERM's ERM practices; and
- Evaluating progress made since IOPA's 2019 Ethics Program Review,[1] including by performing sample testing on Ethics hotline submissions from January 2022 through September 2023 via:

[1] IOPA's Performance Review: Ethics Program Redesign (Nov. 2019).

(1) the evaluation of appropriate intake, processing, and dispositioning; and (2) the verification of appropriate user access.

The scope of IOPA's Review excluded the following areas:

- Information Security Governance, which moved from OERM to ODST in July 2023; and
- Except as detailed above, comprehensive Ethics coverage, which IOPA presently intends to include in a future program review.

IOPA conducted this Review in conformance with The Institute of Internal Auditors' (The IIA) *International Standards for the Professional Practice of Internal Auditing.*

1.2 Program and Review Background

Program Background: The Board created OERM in furtherance of the PCAOB's 2018 – 2022 Strategic Plan;[2] in February 2019, the PCAOB hired its first Chief Risk Officer (CRO) to head the newly created office, and Ethics moved from OGC to OERM. In addition to ERM and ECP, OERM's responsibilities also encompass the PCAOB's BCP.

Generally, OERM aims to provide policies, guidance, and a framework for D/Os to better identify, assess, manage, and mitigate risks, and to provide a more holistic view of internal and external risks facing the organization. OERM also serves as a consulting resource for the organization for risk-based projects and initiatives. From IOPA's perspective, since inception OERM has been a leading organizational resource supporting the PCAOB's mission and values. Additional information about OERM includes:

Enterprise Risk Management: The goal of OERM's ERM program is to strengthen the risk management culture across the PCAOB using principles of risk identification, assessment, management, mitigation, and monitoring. The ERM program is designed to provide the Board with a more holistic view of risks facing the PCAOB, along with responses to those risks, and to provide a framework for D/Os to better identify, monitor, measure, manage, and mitigate risks. OERM employs a variety of methods to identify and inform the organization about risk, including routine discussions with Board members, D/O leadership, and Risk Liaisons[3] and reviewing available organizational information like risk metrics and risk event monitoring.

Ethics and Compliance Program: The ECP's goal is to promote an ethical organizational culture by providing leadership, training, and advice on ethics-related matters; developing policies and guidance related to ethics and compliance; and monitoring, coordinating, and investigating ethics-related improprieties, complaints, and allegations (including those reported through the PCAOB Hotline). Ethics is also responsible for administering annual staff ethics certifications and financial disclosure filings.

Business Continuity Program: The purpose of the BCP is to enhance the resiliency of organizational operations in the face of disruptions. The BCP manages the development and maintenance of D/O business continuity plans; the identification of critical functions, applications, data, and associated

[2] *See* PCAOB's 2019 Annual Report at 13 ("In 2019, the Board created a new Office of Enterprise Risk Management (OERM) to transform the PCAOB's approach to risk management and implement the Board's strategic objective of implementing an Enterprise Risk Management program").

[3] Risk Liaisons serve as points of contact within each D/O. Risk Liaisons function as risk partners for OERM and help promote risk awareness within their own D/Os, including by reporting and confirming all risk events on behalf of the respective D/O.

recovery time objectives; implementation of contingency safeguards and procedures to mitigate risks; and on-going preparedness training and testing for potential disruptions. As part of the BCP, OERM also co-leads the organization's Crisis Management Team and Security Incident Response Team.

From 2020 into 2022, OERM led the PCAOB's COVID-19 response, including return-to-work planning and other health and safety proposals and recommendations. OERM continues to serve as a consultant on COVID-19 related issues.

Review Background: This Review is the first time IOPA has performed a comprehensive review of the OERM function. In 2019, IOPA performed a "blueprint" performance review to evaluate ECP's future state; IOPA reviewed the 2019 findings as part of this Review.

1.3 Review Opinion

IOPA's Review found that, in a relatively short five-year period, OERM has done a commendable job in creating and growing a sophisticated second line ERM function, consistent with The IIA's *Three Lines Model*, which promotes structured communication and collaboration between an organization's first line (operating management), second line (specialists assisting first line with managing risk), and third line (independent internal audit function). Generally, OERM has created well-documented guidance and procedures, as well as a comprehensive organizational risk register and detailed risk reporting. The Office has established strong lines of communication and frequent engagement with D/Os. Additionally, OERM has been recognized throughout the organization for its crucial work and leadership responding to COVID-19, which was both essential and effective in supporting the PCAOB during an unprecedented period. In interviewing a variety of OERM Collaborators during Review fieldwork, IOPA generally found respect for and appreciation of OERM's function and activities throughout the organization. Section 1.3.3 below summarizes OERM's leading practices.

During the Review, IOPA identified certain enhancement opportunities that will enable OERM to continue ably supporting the organization. Section 1.3.1 below summarizes the Review observations on a risk scale, which is described in Appendix A, IOPA's Risk Rating Legend.

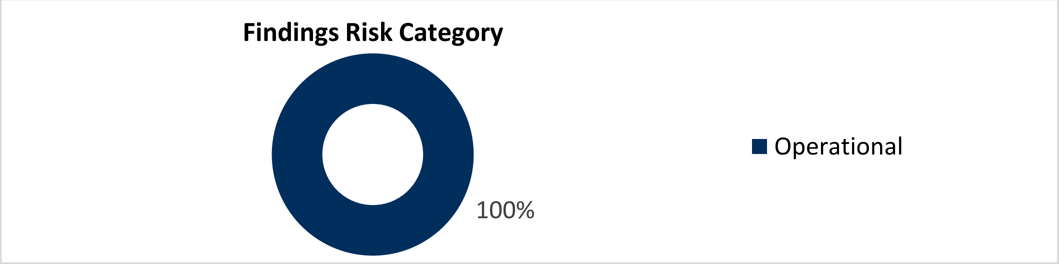
1.3.1 Summary of Review Observations

Observation Summary and Recommendations	Risk Rating	Responsible Party	Target Date
Continue to Enhance the Maturity of the OERM Program After five years of development and growth, OERM has an opportunity to add enhanced value to the PCAOB by further strengthening its second line role of expertise, support, monitoring, and challenge on risk-related matters.[4] IOPA recommends that, with sustained support and visibility from organizational leadership, OERM: (1) further define and communicate the differences between first line and second line roles and responsibilities; (2) continue to look for opportunities to provide supplemental expertise and credible challenge to the PCAOB's first line; and (3) provide greater awareness to the organization of these enhancements and others incorporated by OERM to date.	**Low**	CRO	June 30, 2025
Report OERM's Assessment of Its Own Remedial Activity Only After IOPA's Agreement IOPA notes an opportunity to eliminate a structural conflict in OERM's second line tracking of its first line functions' remediation of IOPA review recommendations. IOPA recommends that, in the limited circumstance where OERM/Ethics is the first line function under IOPA review, OERM completes its first line remedial efforts and then notifies IOPA of the status, after which IOPA will conduct a third line review of the remedial activities. In light of the structural first/second line overlap, OERM's second line tracking reports should not inform the Board and D/Os of the reasonableness of the Office's own first line remedial activity prior to IOPA's review and agreement.	**Low**	CRO	September 30, 2024

[4] *See* The IIA's *Three Lines Model* (July 2020); *see also* The IIA's *Global Perspectives & Insights, Internal Audit and Compliance: Clarity and collaboration for stronger governance* (Jan. 2022) ("First and second line roles constitute management. They reflect the responsibilities of the first line to provide the products and services to clients, and the second line to provide specialist oversight, assess risk (particularly on a collective or portfolio basis), and perform risk management activities, credibly challenging the first line").

1.3.2 Risk Category Distribution

IOPA found that all risks identified during the Review stemmed from operational issues.



1.3.3 Leading Practices

During the Review, IOPA found that OERM has implemented the following leading practices:

- OERM has generated a large volume of foundational documents addressing a wide range of the Office's responsibilities.[5]
- OERM has provided detailed training for OERM Collaborators.
- OERM has been effective in proactively promoting risk awareness across the organization (e.g., Town Hall meetings, training at DRI's Annual Inspections Training, the 2023 inaugural Risk Awareness Week guidance posted on myPCAOB, a 2023 OERM open house event).

1.3.4 Management Response Summary

OERM provided responses indicating a commitment to actions that are responsive to IOPA's recommendations.

IOPA thanks all personnel who supported this Review, both at the senior management and staff operating level, for their courtesy and cooperation throughout this assessment.

[5] OERM's foundational documents include risk event program material and escalation procedures, information memos, strategy documentation, and presentations/briefings to various stakeholders (e.g., Board members, Management Committee, Risk Liaisons, and the U.S. Security and Exchange Commission's Office of the Chief Accountant).

Appendix A, Risk Classification and Definitions

To provide the reader with further perspective of the degree of risk IOPA attributes to each review observation, IOPA has assigned color-coded risk ratings as explained in the legend below.

Material	The degree of risk is unacceptable and poses a significant level of financial, compliance, or operational risk to the organization. As such, complete remediation is generally required on a highest priority basis.
Significant	The degree of risk is undesirable and poses a significant financial, compliance, or operational risk to the organization. As such, complete remediation is generally required on a high priority basis.
Moderate	The degree of risk is undesirable and poses a moderate financial, compliance, or operational risk to the organization. As such, complete remediation is generally required on a medium priority basis.
Low	The degree of risk appears reasonable but there are opportunities to further reduce risk through improvements to existing policies, procedures, and/or operations. As such, on a lower priority basis, management should take actions to reduce the risks to the organization.

IOPA used its professional judgement in determining the overall ratings presented in this report, which is intended to provide management with information about the condition of risks and internal controls at a point in time.