PCAOB
PUBLIC COMPANY ACCOUNTING
OVERSIGHT BOARD

November 12, 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) Performance Review Report: *Office of Technology Change Management* (November 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 ("Review") in conformance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

The purpose of IOPA's Review was to evaluate the efficiency and effectiveness of the PCAOB's information technology (IT) change management processes and controls, which are implemented and managed by the Office of Technology (OT). The scope of IOPA's Review primarily focused on operating policies, procedures, and controls in place from January 2023 through June 2024.

As the attached summary report sets forth, IOPA's Review found that OT has IT change management processes and controls in place that efficiently and effectively process changes to PCAOB systems. The PCAOB's Change Control Board, which IOPA found is appropriately composed of key stakeholders with expertise in various IT disciplines, utilizes sufficient processes and controls to review and approve change requests. Additionally, IOPA found that OT seeks to continuously improve processes, controls, and systems to mitigate significant risks, particularly those related to key systems.

During the Review, IOPA identified certain enhancement opportunities to help enrich OT's support of the organization. *First*, recognizing that IOPA's detailed testing of change requests under current change management policies did not identify instances of non-compliance, IOPA identified opportunities for OT to enhance the efficiency and effectiveness of certain enumerated change management controls and the related documentation. Specifically, IOPA recommends that OT enhance certain change management control processes. *Second*, IOPA believes opportunities exist for OT to enhance and update change management-related documentation. *Finally*, IOPA believes opportunities exist for OT to convey enhanced information to OT stakeholders and decision makers through OT's change request forms, and thus recommends OT enhance the change request form template.

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 November 19, 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 Summary Public Performance Review Report: *Office of Technology Change Management* (November 2024)

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

# Office of Internal Oversight and Performance Assurance

## **Performance Review: *Office of Technology Change Management Review* Summary Report (November 2024)**

## 1. Executive Summary

As detailed herein, from April 2024 through August 2024, the Public Company Accounting Oversight Board's (PCAOB or "Board") Office of Internal Oversight and Performance Assurance (IOPA) conducted a review of the organization's information technology (IT) change management policies and practices ("Review"). The Office of Technology (OT) is tasked with assisting the PCAOB in implementing and managing IT change management processes and controls and ensuring that these processes and controls are sufficiently robust and effective.

### 1.1. Review Objective and Scope

#### Objective

The purpose of IOPA's Review was to evaluate the efficiency and effectiveness of IT change management processes and controls.

#### Scope

The scope of IOPA's Review primarily focused on operating policies, procedures, and controls in place from January 2023 through June 2024. IOPA's field work included:

- Reviewing policies and procedures related to IT change management;
- Gaining an understanding of the processes and people involved in making and testing changes to PCAOB systems;
- Evaluating processes for the promotion of software changes from test environments to production; and
- Assessing OT's remediation efforts in response to a review of an IT system that supports the PCAOB's Division of Registration and Inspections (DRI).

The scope of the Review excluded project management, project budgeting, requirements gathering, and other aspects of IT and other system implementation projects separate from the scope outlined above, all of which IOPA separately examines within system implementation reviews.

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

## 1.2. Program and Review Background

### Program Background

The PCAOB employs both enterprise-wide and department-specific IT systems to support the execution of its mission. The consistent and dependable operation of these systems, in alignment with business requirements, is critical to the accomplishment of the organization's mission.[1] Further, as IT solutions change and business needs evolve, the PCAOB must maintain robust, efficient, and effective IT change management processes and controls to ensure risks are mitigated to acceptable levels.

The *PCAOB Production Change Management Process Narrative* (last updated May 2023) notes that "the PCAOB has a mature change management process that comprises a change request workflow, a Change Control Board (CCB) to evaluate the impact of proposed changes, and a change reconciliation process for those applications that fall under Internal Controls for Financial Reporting (ICFR) control to monitor changes to its production environment."

### Review Background

Effective IT change management is critical to the PCAOB's mission, as technology is a foundational tool used by all staff members to help accomplish the Board's mission. IOPA incorporates this criticality into its annual Risk Assessment and has placed it among the significant organizational risks to evaluate during 2024 through the current Review.

The IIA notes that IT change management is the systematic set of processes that are executed within an organization's IT function to manage enhancements, updates, installations, implementations, incremental fixes, and patches to production systems, and includes:

- system upgrades (e.g., applications, operating systems, and databases);
- infrastructure changes; and
- security changes.[2]

The IIA further points out that effective change management "can assist an organization in addressing risk, reducing unplanned work, limiting unintended results, and ultimately improving the quality of service for internal and external parties." Risks reduced by effective IT change management include:

- failing to comply with regulations, standards, and policies;
- disruptions in IT services;
- unauthorized changes to production systems;
- changes not being recorded and/or tracked; and
- inappropriate implementation of emergency changes.

[1] *See* The IIA's Practice Guide: IT Change Management (Feb. 2021) ("In the current business environment, a well-thought-out and systematic change management process is no longer optional; rather, it is necessary for an organization to effectively achieve its business objectives").

[2] *Id.*

According to the IIA, effective change management hinges on implementing preventive,[3] detective,[4] and corrective[5] controls.

## 1.3. Review Opinion

Generally, IOPA's Review found that OT has IT change management processes and controls in place that efficiently and effectively process changes to PCAOB systems. The PCAOB's Change Control Board, which is appropriately composed of key stakeholders with expertise in various IT disciplines, utilizes sufficient processes and controls to review and approve change requests. Additionally, IOPA found that OT seeks to continuously improve processes, controls, and systems to mitigate significant risks, particularly those related to key systems.

During the Review, IOPA identified certain enhancement opportunities to help enrich OT's support of 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 Observations

| Observation Summary and Recommendations | Risk Rating | Responsible Party | Target Date |
|---|---|---|---|
| **Enhance Change Management Control Processes**<br>Recognizing that IOPA's detailed testing of change requests under current change management policies did not identify instances of non-compliance, IOPA identified opportunities for OT to enhance the efficiency and effectiveness of certain enumerated change management controls and the related documentation. Specifically, IOPA recommends that OT enhance its change management control processes in this area. | **Low** | OT | April 2025 |
| **Enhance Change Management Documentation**<br>IOPA believes opportunities exist for OT to enhance and update change management-related documentation. | **Low** | OT | June 2025 |

[3] *Id.* Preventive controls "deny certain changes unless specific actions or conditions are met," such as appropriate authorizations, segregation of roles/duties, completion of minimum required steps, appropriate and complete documentation of changes (i.e., description, risk, systems impacted, rollback/backout plan), and appropriate permissions being in place.

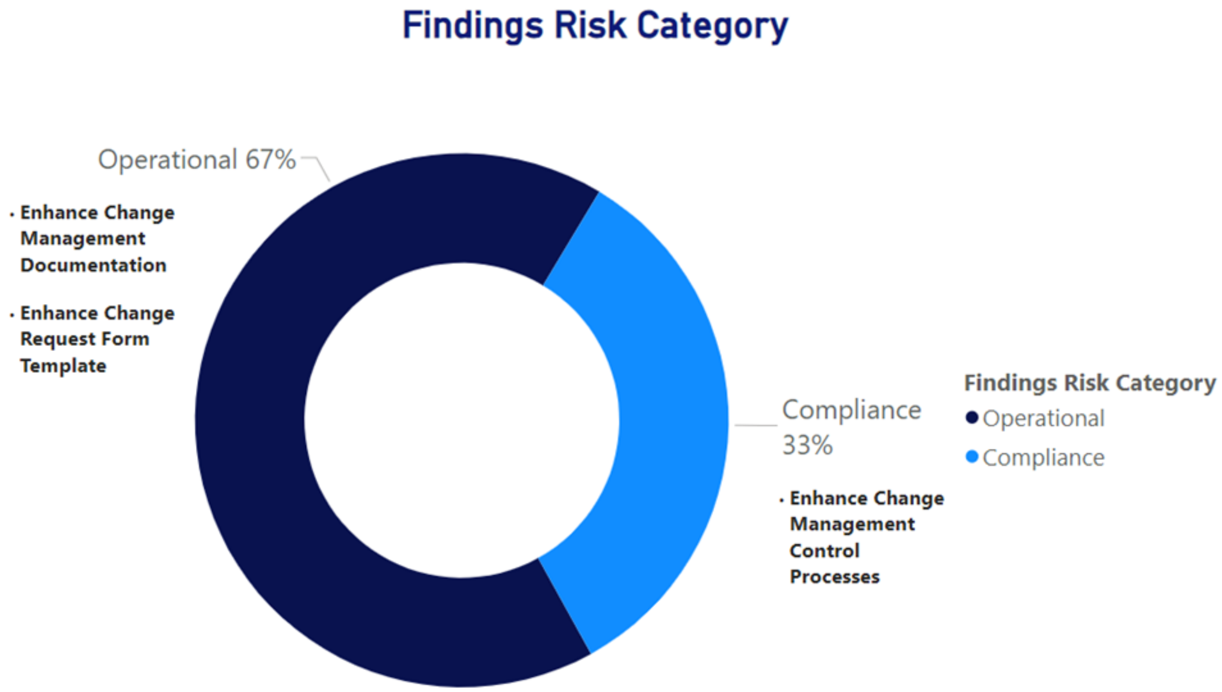
[4] *Id.* Detective controls help "monitor completed changes to determine if any undesirable changes or unintended outcomes have occurred," and can include detection of unauthorized or incorrectly authorized changes and monitoring of valid, objective change management metrics.

[5] *Id.* Corrective controls are "predetermined actions taken when certain post-change conditions or behaviors are found. These controls could include: • Post-implementation reviews. • Change information fed into early problem diagnosis steps."

| Observation Summary and Recommendations | Risk Rating | Responsible Party | Target Date |
|---|---|---|---|
| **Enhance Change Request Form Template**<br>IOPA believes opportunities exist for OT to convey enhanced information to OT stakeholders and decision makers through OT's change request forms, and thus recommends OT enhance the change request form template. | **Low** | OT | June 2025 |

### 1.3.2 Risk Category Distribution

IOPA found that risks identified during the Review related mostly to operational issues (*see* Observations 2 and 3), but IOPA also noted potential compliance risks related to change management controls (*see* Observation 1).



### 1.3.3 Leading Practices

As noted above, IOPA found that OT seeks to continuously improve processes and systems to mitigate significant risks, particularly those related to key systems. Relatedly, IOPA's Review identified OT's implementation of numerous leading practices, including:

- Initiating a project to create a consolidated and comprehensive list of IT controls, including change management controls;
- Implementing new change management controls around a specific DRI system, including controls that leverage automation to identify potential risks;
- Developing Security and Privacy Impact Assessment (SPIA) template documentation by leveraging guidance and templates from the National Institute of Standards and Technology;[6] and
- Incorporating guidance from the Office of Management and Budget (OMB) for the privacy impact assessment portion of the SPIA template.[7]

### 1.3.4 Management Response Summary

OT provided responses indicating a commitment to actions that are responsive to our recommendations.

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

[6] *See* Guide for Security-Focused Configuration Management of Information Systems, Special Publication 800-128, Appendix I. SPIAs are used for projects or change requests with potentially significant modifications as to security and privacy of information.

[7] Although the PCAOB is not a federal agency and thus not required to follow OMB guidance, IOPA believes that incorporating OMB guidance as part of the privacy impact assessment portion of the SPIA aligns with leading practices.

# Appendix A - Risk Classification and Definitions

To provide the reader with further perspective of the degree of risk IOPA attributes to each review observation and 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 judgment 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.