Paschal Mmesoma Ezeliora
Seattle, Washington
July 28, 2026

Via email: comments@pcaobus.org

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street, NW
Washington, DC 20006-2803

Re: Request for Public Comment on PCAOB Standard Setting (PCAOB Release No. 2026-005, June 23, 2026)

Dear Office of the Secretary:

I respectfully submit this comment in response to the Board's Request for Public Comment on PCAOB Standard Setting (Release No. 2026-005, June 23, 2026). Rather than address all twenty-four questions, this letter responds in depth to the questions on which my practice gives me a concrete basis to comment: Questions 1, 2, 4, 8, and 10. Section A describes my background. Section B addresses data and technology, including artificial intelligence, as a standard-setting priority (Questions 1, 2, 8, and 10). Section C addresses the fraud project and AS 2401 (Questions 1, 2, and 4). Section D concludes.

A. Commenter Background

I am an internal audit practitioner and researcher with financial-controls experience across banking, professional services, and technology-sector environments. I have co-authored published papers on machine-learning applications in supply-chain risk management, encryption and financial-data security in financial technology, and empirical-finance topics, and I am developing an open practitioner framework of test procedures, control checklists, and risk matrices for AI-assisted audit evidence and automated supply-chain financial flows. I am commenting because the questions this Request raises about data, technology, and fraud are the questions my field-level work addresses, and because audit quality, investor protection, and the reliability and integrity of financial reporting depend on closing the gap between AI governance frameworks and audit field procedures.

B. Data and Technology, Including Artificial Intelligence, Should Be a Priority for Standard Setting (Questions 1, 2, 8, and 10)

I support the Board's identification, in Table 1 of the Request, of the need to “Consider changes related to data and technology, including artificial intelligence and digital assets, as a critical emerging issue relevant to the development of the PCAOB's strategic priorities” (Release No. 2026-005, p. 6), and I urge the Board to prioritize this area for both research and standard setting (Question 1). My reason is a specific, observable gap. At the objective level, the governance frameworks now exist. NIST's AI Risk Management Framework “describes four specific functions to help organizations address the risks of AI systems in practice. These functions – GOVERN, MAP, MEASURE, and MANAGE – are broken down further into categories and

subcategories" (NIST AI 100-1, January 2023, p. 8). NIST's Generative AI Profile defines the failure modes that matter most for audit evidence, including "Confabulation: The production of confidently stated but erroneous or false content (known colloquially as 'hallucinations' or 'fabrications')…" (NIST AI 600-1, July 2024, p. 8). COSO's guidance on internal control over generative AI likewise identifies the control conditions, observing that "adoption is easy enough that 'shadow AI' (unauthorized or ungoverned AI implementations operating outside formal IT oversight) can start outside formal channels" and that "Explainability and transparency. Opaque reasoning frustrates validation, testing, and stakeholder confidence" (COSO, Achieving Effective Internal Control Over Generative AI, February 2026, pp. 5–6).

What does not yet exist is the corresponding field-procedure layer: authoritative direction that tells an engagement team what it must test, corroborate, and document before relying on evidence that an AI system produced or touched. The Board's own staff observed in July 2024 that "The integration of GenAI in audits and financial reporting is in its early stages but rapidly evolving" (PCAOB staff, Spotlight: Generative AI in Audits and Financial Reporting, July 2024, p. 4). My experience is consistent with that observation, with one addition: deployment is running ahead of procedure. Engagement teams can name the framework functions and the risk classes; they cannot yet point to authoritative criteria for what those objectives require of a specific procedure on a specific engagement. The scope of a data-and-technology project should therefore be the field-procedure level (Question 2): requirements, or at a minimum detailed staff guidance, that translate framework-level objectives into engagement-level testing and documentation.

Question 8 asks which instrument should carry this work. In my view, the highest-priority need is staff guidance on the sufficiency of AI-generated evidence. Firms are already deploying these tools at scale, yet engagement teams lack practical criteria under AS 1105, Audit Evidence, for determining when an AI-produced output constitutes sufficient appropriate audit evidence. Of the matters prior commenters have identified (the impact of a company's use of AI on risk assessment, auditing internal controls, sufficient appropriate audit evidence, documentation, and supervision of AI-assisted work), evidence sufficiency is the one on which engagement teams need direction most urgently, because it is a judgment they are already making daily without criteria. Staff guidance can reach the field fastest; standard setting on the same subject should follow as the durable instrument.

Question 10 asks which existing standards may not be fit for purpose in the current environment. Two stand out from my practice:

1. AS 1105, *Audit Evidence*. The standard was written for traditional forms of evidence and provides almost no framework for evaluating the reliability, completeness, or appropriateness of AI-generated outputs. Engagement teams currently lack clear criteria for when AI-produced analyses, samples, or narratives constitute sufficient appropriate audit evidence. The Board should add explicit requirements, or at a minimum detailed application guidance, addressing: (a) evaluation of the data and the model underlying an AI-generated output; (b) validation of the output itself; and (c) the circumstances in which AI-generated information can, and cannot, be used as audit evidence without significant additional procedures.

2. AS 1201, *Supervision of the Audit Engagement*. The standard assumes traditional human work product and hierarchical review; it does not address how a partner or manager should direct, supervise, and review work that was substantially performed or assisted by AI tools.

The Board should require the engagement team to document: (i) how AI tools were directed and constrained; (ii) the nature and extent of the review performed over AI outputs; and (iii) how professional skepticism was applied specifically to AI-assisted procedures.

C. Fraud and AS 2401 (Questions 1, 2, and 4)

The Request's fraud row asks the Board to "Consider whether AS 2401, Consideration of Fraud in a Financial Statement Audit, should be revised and, if so, how" and to "Consider how AS 2401 could better align an auditor's responsibilities for addressing intentional acts that result in material misstatements in financial statements with the auditor's risk assessment, including addressing matters that may arise from developments in the use of technology" (Release No. 2026-005, p. 6).

Recommendation 1: evidence produced or touched by AI systems. A modernized fraud standard should require that, before relying on audit evidence that an AI system produced or materially processed, the auditor should: (1) obtain and document the provenance of the AI-produced evidence, including the model and version used, the inputs, prompts, or parameters supplied, the data sources that fed the output, and who controlled those inputs; (2) trace the output to the underlying reliable source data or documents the system used, or claimed to use; (3) re-perform, on a defined sample, the key calculations, classifications, or extractions independently, or with a different tool, to test whether the output is accurate and complete; and (4) reach and document an explicit conclusion: rely, corroborate with additional procedures, or do not rely. These four steps together form the practical minimum; none of them alone is sufficient.

This requirement should be scaled to risk. The full set of procedures should apply where AI-produced evidence supports a significant assertion (existence, completeness, valuation, rights and obligations, or presentation) for a material account or disclosure. For low-risk items that are not material, provenance documentation together with limited sample re-performance may be accepted. Where a system offers no usable provenance, or the entity cannot provide the source data, the auditor should treat the output as unsupported and design alternative procedures. Re-performance sample sizes should be risk-based, increasing for complex models, high-volume transaction flows, and areas with known risk of confabulated or otherwise erroneous output.

Recommendation 2: automated, high-volume supply-chain financial flows. Where invoices, receivables, or related financing instruments flow through automated systems at volume, the fraud standard should require the auditor to: (1) perform cross-system matching of the automated records back to the original source instruments (purchase orders, shipping documents, contracts, bank confirmations, and similar records) on a risk-based sample; (2) test for alteration and duplication, including duplicate-invoice detection, modification of key fields after initial recording, and unusual patterns that automated controls may miss; and (3) specifically identify and reconcile supply-chain financing arrangements, including those that are off-balance-sheet or structured through third-party platforms, and evaluate whether the related accounting and disclosure are appropriate. Automated processing at volume can allow altered, duplicated, or unsupported instruments to pass review; the procedures above are directed at that failure mode.

Recommendation 3: closing the deployment gap in proactive detection controls. The empirical case is documented. The ACFE's Occupational Fraud 2026: A Report to the Nations finds that "targeted anti-fraud controls such as job rotation and mandatory vacation policies,

surprise audits, and proactive data monitoring and analysis were all in place at fewer than half of the victim organizations…" (p. 38). The same report identifies two controls it associates with at least a 50% reduction in median fraud losses: proactive data monitoring and analysis ("49% of organizations had this control in place," associated with a "53% reduction of median fraud losses") and surprise audits ("44% of organizations had this in place," associated with a "50% reduction in fraud losses") (p. 47). In other words, the controls the report associates with these loss reductions were absent from more than half of the victim organizations.

A modernized AS 2401 should direct the auditor's attention to exactly that gap. I suggest requirement language along the following lines: "In identifying and assessing the risks of material misstatement due to fraud, the auditor shall specifically evaluate the presence or absence of proactive detection controls (including, but not limited to, surprise audits, data analytics monitoring, and independent verification processes) that have been shown to significantly reduce fraud losses, and shall document how the presence or absence of such controls affected the assessed risks and the nature, timing, and extent of further audit procedures." The purpose of the requirement is to move the fraud risk assessment beyond the traditional inquiries and brainstorming, and to make the auditor actually consider whether the entity has the controls the data show to work, with a documented link from that evaluation to the further procedures performed.

Question 4 asks about the prioritization of the remaining interim standards. AS 2401 appears in the Request's Appendix 1 list of interim standards adopted in 2003 and "in effect substantially in the form adopted" (Release No. 2026-005, p. 18). It should rank in the top tier, among the first three interim standards modernized. Fraud risk assessment remains foundational to the audit, yet the current standard does not adequately address AI-generated evidence, high-volume automated transaction flows, or the well-documented under-deployment of the most effective detection controls.

D. Closing

The recommendation I most want to leave with the Board is this: advance the data-and-technology project and the AS 2401 fraud project together, because AI-era audit evidence and fraud detection are one problem surface. Evidence that an AI system produced or touched, and fraud that automated volume can conceal, are evaluated by the same engagement teams under the same standards; modernizing one without the other would leave the field with half a toolkit. I thank the Board for the opportunity to comment and for its attention to these matters, and I am available by email for any follow-up questions the Board or its staff may have.

Respectfully submitted,

Paschal Mmesoma Ezeliora
Internal audit practitioner and researcher
paschalezeliora@gmail.com

This comment is submitted in my personal capacity. The views expressed are my own and do not represent the views of any employer, client, or organization.