Comment Letter on PCAOB Strategic Priorities (PCAOB No. 2026-001)

Jake Sigler, Ph.D.

Xavier University

I. Introduction

I appreciate the opportunity to provide input on the PCAOB strategic priorities for its 2026–2030 strategic plan. My perspective is informed by academic research on audit quality and technology, as well as prior experience as a PCAOB Research Fellow.

This comment letter focuses on the implications of increasing technology complexity and artificial intelligence ("AI") for audit risk, audit evidence, and the role of IT expertise within the audit process. The central point is that technology, particularly AI, is increasing audit risk, changing the nature of audit evidence obtained and generated in the audit process, and altering how the PCAOB can most effectively conduct inspections. As a result, the PCAOB's strategic priorities should emphasize modernization of audit evidence standards, risk assessment frameworks, and inspection approaches to reflect these changes.

II. Executive Summary

- Technology complexity increases audit risk; auditors identify this risk and increase effort, but residual risk remains
- Risk enters the audit through two channels: issuer-side technology complexity and auditor-side use of analytics and AI
- AI shifts the nature and where audit risk arises and changes what constitutes audit evidence
- Auditors should expand evaluation of evidence to include dimensions such as truthfulness, traceability, explainability, and reproducibility
- Standards should remain technology-neutral while being updated to address technology-driven evidence and risk (AS 1105, AS 2110, AS 2301)
- IT audit expertise is central to audit quality and should be integrated throughout the audit process
- The PCAOB can use AI to perform an initial, within-engagement screening of documentation to identify higher-risk areas, improving efficiency while maintaining inspector judgment through appropriate guardrails

III. Technology Complexity, AI, and Audit Risk

Prior research shows that increases in IT complexity are associated with higher audit risk, and that auditors generally recognize this risk during planning and respond by increasing overall

audit effort (Choudhary, Sigler, and Ramadas 2025). However, additional effort does not fully offset the risk. More complex engagements exhibit higher rates of inspection findings, financial reporting issues, and failed audit engagements. These patterns indicate persistent residual risk in technology intensive settings and suggest that traditional audit approaches are not sufficient to fully mitigate complexity driven risk. Importantly, this evidence suggests that increasing audit effort alone is not sufficient to address risks arising from complex and technology-enabled environments.

These risks arise through two distinct but related channels. First, issuer side technology complexity increases the difficulty of understanding systems, tracing data, and evaluating controls within financial reporting processes. Second, the auditor's use of advanced analytics and AI introduces additional complexity within the audit itself, as evidence is generated, transformed, and evaluated through automated and model driven processes.

The adoption of AI further intensifies both channels. AI systems introduce additional layers of complexity, including non deterministic outputs, opaque processing logic, and evolving data dependencies (Issa, Sun, and Vasarhelyi 2016). Accordingly, AI should be viewed not as a discrete tool, but as a new layer of complexity embedded within both the issuer environment and the audit process.

Importantly, the addition of technology shifts the nature and where audit risk arises, changing not only how audits are performed, but also what constitutes audit evidence. In many cases, audit evidence will be generated, transformed, or summarized by AI systems rather than directly observed. Auditors must therefore evaluate the reliability of system generated representations of underlying economic activity.

Current PCAOB standards were developed in an environment where audit evidence was largely static, systems were more transparent, and data flows were more easily traceable. As a result, existing guidance focuses primarily on completeness and accuracy of underlying data, with less emphasis on how evidence is generated, transformed, and interpreted within complex, technology driven systems. In AI enabled environments, these assumptions no longer hold. Evidence may be produced through opaque processing logic, incorporate evolving data inputs, and reflect outputs that are not directly reproducible or easily explainable. This gap between existing standards and the realities of modern technology environments underscores the need for guidance that explicitly addresses how issuer complexity and auditor use of AI affect the reliability of audit evidence.

The PCAOB has already recognized the importance of these issues through its Data and Technology research project, which evaluates whether changes to auditing standards or additional guidance are needed in response to the increasing use of technology by auditors and preparers. Building on this work, the analysis above suggests that these efforts should focus specifically on how technology shifts the nature of audit evidence and introduces new forms of audit risk that are not fully addressed under current standards.

IV. Exhibit 1: Technology-Driven Audit Evidence Risk Framework

Figure 1 illustrates how audit risk arises across inputs, processing, and outputs in technology-enabled environments. The framework reflects two distinct but related channels through which risk enters the audit: issuer-side technology complexity and auditor-side use of analytics and AI. Together, these channels highlight the need to evaluate evidence beyond traditional completeness and accuracy considerations.

V. Figure 2: AI-Enabled Inspection Screening Within Engagements

Figure 2 illustrates how the PCAOB could use AI as an initial screening layer over engagement documentation to identify higher-risk areas within engagements. The figure depicts (i) ingestion of workpapers and audit documentation, (ii) feature extraction (e.g., coverage vs. risk alignment, data lineage signals, documentation completeness), (iii) model-based scoring of sections/areas, and (iv) inspector review where AI outputs guide, but do not replace, professional judgment. The objective is to improve efficiency and targeting by directing inspectors to areas most likely to exhibit detection risk, with appropriate guardrails to ensure outputs are treated as risk indicators rather than conclusions.

Exhibit 1: Technology-Driven Audit Evidence Risk Framework

Audit Risk Across Inputs, Processing, and Outputs in Technology-Enabled Enviroments

Audit risk arises through two interrelated channels: issuer-side technology complexity and auditor-side analytics and AI (TBATs). These channels jointly affect the reliability of audit evidence and require evaluation beyond completeness and accuracy.

CHANNEL 1: ISSUER-SIDE TECHNOLOGY COMPLEXITY
The data environment that produces audit evidence (inputs)

CHANNEL 2: AUDITOR-SIDE ANALYTICS, AI, AND TBAT USE
The audit procedures and tools that generate and analyze evidence (processing)

1 INPUTS – ISSUER-SIDE TECHNOLOGY COMPLEXITY
(Data Environment and Source Systems)

Systems & Applications | Data Sources & Databases | Data Flows & Interfaces | IT Complexity & Dependencies

Issuer-generated data environments, including underlying systems, applications, data flows, and IT complexity that produce audit evidence.

AUDIT FOCUS

- **Completeness** – Are all relevant data sources captured?
- **Accuracy** – Are source systems and data reliable?
- **Traceability** – Can data be reconciled to underlying systems and processes?
- **Data Integrity** – Are transformations and extractions free from distortion?

KEY RISK
Complex, fragmented, or poorly controlled IT environments produce biased, incomplete, or unreliable inputs, which propagate through the audit.

2 PROCESSING – AUDITOR-SIDE ANALYTICS, AI, AND TBATs
(Execution of Audit Procedures and Evidence Generation)

Analytics | Automation | Data Validation | TBATs / AI Tools

Auditor-generated evidence through analytics, automation, and technology-based audit tools (TBATs), including AI-enabled procedures.

AUDIT FOCUS

- **Logic Integrity** – Do analytics and TBATs function as intended?
- **Assumptions & Model Design** – Are models appropriate, documented, and valid?
- **Appropriateness** – Are tools suitable for the audit objective and data context?
- **Tool Performance (TBATs)** – Do tools produce reliable outputs under varying conditions?
- **Human Oversight** – Is there sufficient auditor review and skepticism applied to automated outputs?

KEY RISK
Flawed logic, invalid assumptions, or inappropriate TBAT use may lead to undetected misstatements or systematically biased evidence, even when inputs are reliable.

3 OUTPUTS – EVALUATION AND AUDITOR JUDGMENT
(Evidence Interpretation and Conclusions)

Results | Corroboration | Conclusions

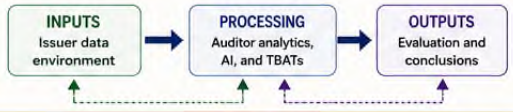
Evaluation of results, corroboration with other audit evidence, and formation of audit conclusions.

AUDIT FOCUS

- **Completeness** – Are all relevant results evaluated?
- **Accuracy** – Are outputs correct and free from error?
- **Reasonableness** – Do results reflect economic reality?
- **Truthfulness** – Do conclusions faithfully represent underlying conditions?

KEY RISK
Overreliance on outputs without sufficient professional skepticism or corroboration may result in misleading conclusions, even when procedures appear robust.

FRAMEWORK INSIGHT
Audit risk in technology-enabled environments is not confined to evidence evaluation. It emerges from the interaction between issuer-side complexity shaping the data (inputs) and auditor-side technology shaping the analysis (processing). As a result, audit evidence must be evaluated across the full pipeline, not solely on traditional attributes such as completeness and accuracy.



LEGEND
- Issuer-Side Channel (Inputs)
- Auditor-Side Channel (Processing)
- Common Endpoint (Outputs)
- Interrelated Risk Flow

IMPLICATIONS FOR PCAOB STANDARD-SETTING

- **AS 1105 (Audit Evidence)** – Expand guidance to address reliability of auditor-generated evidence, including TBATs and AI outputs.
- **AS 2110 (Risk Assessment)** – Incorporate issuer IT complexity and data environments as explicit drivers of inherent risk.
- **AS 2301 (Responses to Risks)** – Align audit procedures with risks introduced by analytics, automation, and AI-enabled tools.

This framework supports a holistic approach to audit risk—recognizing that reliable conclusions depend on the quality of both the data environment and the technology-driven audit process.

Exhibit 2: Issuer AI-Generated Evidence Risk Framework

Risk Arises Across the AI Evidence Lifecycle and Affects the Reliability of Issuer-Generated Information

Issuer use of AI systems can introduce misstatement risk into financial reporting.
Risks arise across the AI evidence lifecycle—from data inputs to AI outputs—and must be understood by auditors to evaluate reliability.

Issuer AI Evidence Lifecycle

1 DATA INPUTS	2 AI SYSTEM & MODEL	3 AI PROCESSING	4 HUMAN OVERSIGHT & REVIEW	5 AI-GENERATED EVIDENCE
Data used to train, tune, or run AI systems	Design, training, and configuration	Execution and output generation	Monitoring, validation, and approval	Incorporation into financial reporting
Structured and unstructured data from internal and external sources entering the AI system.	AI models are selected or built, trained or fine-tuned, and configured with parameters and rules.	The AI system processes data and generates outputs, predictions, classifications, or recommendations.	Management reviews AI outputs, monitors performance, and approves results for use in reporting.	AI-generated outputs are used in accounting estimates, disclosures, or other financial statement elements.
KEY RISKS				
• Incomplete or biased data • Poor data quality or integrity • Inadequate data governance • Lack of representativeness	• Flawed model design • Inappropriate model selection • Overfitting or underfitting • Weak documentation and change controls	• Model errors or instability • Processing or coding errors • Sensitivity to unusual conditions • Lack of explainability	• Insufficient review and challenge • Overreliance on AI outputs • Inadequate monitoring • Conflicts of interest or incentives misaligned with accuracy	• Misstatement in estimates or disclosures • Omitted or misleading information • Inappropriate use in financial reporting • Lack of audit trail
AUDIT IMPLICATIONS				
• Understand data sources and lineage • Evaluate data quality and controls • Test completeness and representativeness	• Evaluate model design and appropriateness • Assess training data and assumptions • Inspect documentation and change management	• Test model performance and accuracy • Evaluate robustness across conditions • Assess explainability and limitations	• Evaluate oversight activities and governance • Test monitoring and approval processes • Assess management's challenge and judgment	• Test reasonableness of estimates and disclosures • Reconcile outputs to source data and assumptions • Evaluate completeness and consistency in reporting
EXAMPLES				
• Customer transaction data • Market and economic data • Internal operational data • Third-party data feeds	• Demand forecasting models • Credit risk scoring models • Natural language processing (NLP) for contract analysis • Anomaly detection models	• Revenue prediction outputs • Fair value estimates • Fraud risk scores • Automated journal entry recommendations	• Review by finance / data science teams • Back-testing and validation • Management sign-off • Performance dashboards	• Allowance for credit losses (CECL) • Inventory valuation • Revenue recognition estimates • MD&A narrative disclosures

KEY RISK CHARACTERISTICS

- Complex and opaque ("black box" risk)
- Data-dependent and context-sensitive
- Evolving over time (model drift risk)
- Difficult to detect without specialized techniques
- Can lead to systematic misstatement

IMPLICATIONS FOR PCAOB STANDARD-SETTING

- **AS 1105 (Audit Evidence)** — Provide guidance on evaluating reliability of issuer AI-generated evidence, including AI model risk, data quality, and governance.
- **AS 2110 (Risk Assessment)** — Require auditors to assess risks arising from issuer use of AI, including model design, use, and monitoring risks.
- **AS 2301 (Responses to Risks)** — Require tailored audit procedures for AI-related risks, including use of data analytics, specialists, and testing of models and outputs.

KEY TAKEAWAY

AI-generated evidence from issuers can introduce new and amplified risks that require auditors to expand their evaluation beyond traditional data and control considerations.

VI. Implications for Audit Evidence and Standard-Setting

In technology-enabled environments, traditional audit procedures that emphasize completeness and accuracy remain necessary but are no longer sufficient. This is particularly true given the two channels through which technology-related risk enters the audit: complexity within issuer systems and complexity introduced through the auditor's use of analytics and AI. In AI-enabled settings, auditors face specific risks that are not fully addressed by existing procedures, including model risk, non-deterministic outputs, data lineage breaks, and the potential for system-generated outputs to misrepresent underlying economic activity. These risks can increase detection risk even when audit effort increases, particularly when auditors rely on outputs that are difficult to verify through traditional means. Auditors must therefore expand their evaluation of audit evidence to address these risks by incorporating additional dimensions of reliability, for example:

Dimension	Definition	Risk Addressed	Example Situation	Example Audit Procedure
Truthfulness	Whether outputs faithfully represent underlying economic conditions and are not distorted by model limitations or hallucination risk	Misrepresentation of economic reality due to model error, bias, or hallucinated outputs	AI tool summarizes revenue contracts and introduces incorrect terms or omissions	Independently reconcile AI outputs to source data and known benchmarks; perform reasonableness checks against external evidence
Traceability	Whether data and transformations can be linked across systems and models, particularly where data is aggregated or transformed through multiple processes	Data lineage breaks, incomplete data capture, or loss of audit trail across systems	Data flows from ERP to data lake to analytics tool with undocumented transformations	Perform end to end data lineage testing; trace samples from output back to originating systems and transformations
Explainability	Whether the auditor can understand how outputs are generated and evaluate the appropriateness of underlying assumptions and logic	Opaque model logic leading to inappropriate reliance on outputs that cannot be evaluated	Black box model flags anomalies without clear rationale or feature drivers	Review model documentation, assumptions, and logic; involve IT specialists to assess model design and appropriateness
Reproducibility	Whether outputs can be consistently regenerated under the same conditions, providing assurance that results are stable and not dependent on uncontrolled variation	Unstable or non-deterministic outputs that vary across runs, increasing detection risk	Generative AI produces different exception lists across repeated runs with the same prompt	Reperform procedures using the same inputs and parameters; test for consistency of outputs across multiple runs

PCAOB standards should remain technology-neutral and avoid inadvertently constraining the appropriate use of advanced analytics and AI. At the same time, they should provide clearer guidance on how auditors evaluate the reliability of technology-generated evidence. In particular, standards should more explicitly address how auditors assess risks arising from model driven processing, evaluate the integrity of data flows across systems, and determine whether system generated outputs can be relied upon as audit evidence. Without such guidance, auditors may default to applying traditional procedures that are not designed to address the specific risks introduced by AI-enabled environments.

Accordingly, the PCAOB should prioritize updates to core auditing standards to better align audit procedures with these risks.

- AS 1105 (Audit Evidence) should be expanded to address the reliability of AI-mediated and system-generated evidence, including expectations for evaluating model outputs, underlying data integrity, and the conditions under which such evidence can be considered sufficient and appropriate
- AS 2110 (Risk Assessment) should more explicitly incorporate IT complexity and AI as drivers of inherent risk, including guidance on evaluating system architecture, data dependencies, and the interaction between issuer systems and auditor-deployed technologies
- AS 2301 (Responses to Risks) should provide clearer direction on designing audit procedures that respond to risks introduced by automated processing, including when traditional procedures are insufficient and when alternative procedures, such as model validation, data lineage testing, or re-performance, are necessary

Absent such updates, there is a risk that auditors will continue to apply procedures designed for more transparent and deterministic environments to settings where evidence is generated through complex and opaque systems. This misalignment may increase detection risk despite increased audit effort and technological sophistication.

VII. Role of IT Auditors in Technology-Enabled Audits

Prior research indicates that the effective use of IT audit expertise can mitigate risks associated with IT complexity, particularly when IT auditors are engaged early and possess relevant experience (Choudhary, Sigler, and Ramadas 2025). Evidence also suggests that the use of IT auditors has increased over time, reflecting the growing importance of technology in financial reporting and auditing. As technology becomes more complex and AI adoption expands, IT audit expertise is not merely supportive but a critical component of audit quality.

While PCAOB standards address the use of specialists and internal controls (e.g., AS 1210, AS 1201, AS 2110, and AS 2201), they do not clearly define the role or integration of IT audit expertise within the core audit process. Unlike other specialists, such as valuation or tax experts

who are typically engaged for discrete accounts or specific transactions, IT auditors address risks that are pervasive across the financial reporting environment. Information systems underpin multiple processes, data flows, and controls, meaning IT-related risks affect numerous audit areas simultaneously rather than a single component. As a result, treating IT auditors as episodic or support resources understates their role. In practice, they should function as core contributors to audit risk assessment and evidence evaluation across the engagement.

As technology complexity and AI adoption increase, this ambiguity directly affects audit quality outcomes. Audit quality depends not only on the procedures performed, but on how effectively IT expertise is integrated into planning, execution, and evaluation.

The PCAOB should clarify expectations for:

- When IT audit expertise is required
- How IT auditors are integrated into engagement teams
- How IT-related work is supervised and reviewed

This can be addressed through targeted updates to existing standards, including AS 2110 (Risk Assessment), AS 1201 (Supervision), and AS 1210 (Using the Work of a Specialist).

VIII. Use of Technology by the PCAOB

The PCAOB can leverage AI to perform an initial review of engagement documentation to identify indicators of elevated audit risk and the potential for elevated detection risk or audit deficiencies. Rather than replacing inspection judgment, these tools would serve as a first-pass screening mechanism, efficiently triaging large populations of engagement documentation and highlighting specific areas within engagements that warrant closer inspection based on patterns in workpapers, testing coverage, and documentation quality (e.g., SEC Division of Economic and Risk Analysis 2022; FCA 2022; BIS 2019).

For example, AI could be used to scan engagement documentation to identify gaps or inconsistencies that may indicate incomplete or cursory audit work. This may include situations where audit procedures appear misaligned with assessed risk, such as limited cutoff testing in high-volume revenue environments, omission of high-risk accounts in journal entry testing, or confirmations processes with low response rates and no documented follow-up. It could also identify walkthroughs that do not clearly evidence key control points in complex system environments, or analytics that identify exceptions without corresponding follow-up procedures.

By performing this initial screening, AI can improve inspection efficiency by directing inspectors toward specific areas within engagements with a higher likelihood of detection risk, allowing inspection resources to be allocated more effectively. This is particularly important given the volume and complexity of engagement documentation, which can make it difficult to identify risk signals through manual review alone.

At the same time, it is critical that these tools are implemented with appropriate guardrails. AI outputs should be treated as risk indicators rather than conclusions, and professional judgment by inspectors must remain the primary basis for inspection decisions. When designed and deployed in this way, AI can enhance, rather than replace, the PCAOB's inspection process by improving the consistency and effectiveness of risk identification while preserving the central role of human judgment.

IX. Conclusion

Audit quality risks are increasingly driven by complex, technology-enabled environments. As AI becomes embedded in financial reporting and audit processes, the PCAOB has an opportunity to modernize its standards and oversight to reflect how audit evidence is generated, transformed, and evaluated in practice.

The objective is not to encourage or discourage the use of AI, but to ensure that audit standards appropriately reflect the evolving nature of audit evidence and the expertise required to evaluate it. A focus on technology-neutral standards, enhanced integration of IT expertise, and system-level inspection approaches will better position the PCAOB to fulfill its investor protection mission.

X. References

Choudhary, P., J. Sigler, and V. Ramadas. 2025. *Putting the IT in Audit Risk: IT Complexity and IT Auditor Mitigation.* Working paper.

Issa, H., T. Sun, and M. Vasarhelyi. 2016. Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting* 13 (2): 1–20.

Public Company Accounting Oversight Board (PCAOB). Data and Technology Research Project. Available at: https://pcaobus.org/oversight/standards/standard-setting-research-projects/data-technology

Public Company Accounting Oversight Board (PCAOB). Auditing Standards AS 1105, AS 2110, AS 2301, AS 1201, AS 1210, AS 2201.

Securities and Exchange Commission (SEC), Division of Economic and Risk Analysis. 2022 Annual Report.

Financial Conduct Authority (FCA). 2020. Data Strategy.

Financial Conduct Authority (FCA). 2022. AI Public-Private Forum Final Report.

Bank for International Settlements (BIS). 2018. Supervisory Technology (SupTech) for Prudential Supervision.

Bank for International Settlements (BIS). 2019. SupTech applications and implications.