

PCAOB AI Standards: SOX & ICFR Audits for CFOs & NetSuite

Published May 20, 2026 40 min read



Executive Summary

This report examines the Public Company Accounting Oversight Board's (PCAOB's) evolving stance on artificial intelligence (AI) in the context of Sarbanes–Oxley Act (SOX) compliance and Internal Control over Financial Reporting (ICFR) audits, with a focus on what Chief Financial Officers (CFOs) and NetSuite administrators need to know as of 2026. It reviews recent PCAOB activities, standard-setting, and staff outreach regarding the use of AI and generative AI (GenAI) in financial reporting and audits. It also synthesizes guidance from stakeholder groups such as COSO and international regulators, survey data on CFO attitudes toward AI, and illustrative industry examples.

Key findings include:

- PCAOB Engagement with AI:** The PCAOB is actively monitoring and guiding the intersection of AI and auditing. In 2022–2025 the PCAOB convened a Technology Innovation Alliance (TIA) working group (chaired by Board member Christina Ho) that issued deliverables on emerging technologies. The PCAOB has issued amendments clarifying auditor responsibilities when using technology-assisted analysis (AS 1105 and AS 2301) (Source: pcaobus.org) (Source: pcaobus.org), and in July 2024 released a staff Spotlight on GenAI noting that current use in audits is still mostly limited to administrative tasks but is evolving (Source: pcaobus.org). In September 2025, a PCAOB board member advocated for proactive guidance on AI, including risk-management frameworks and more “agile” audit standards to keep pace with innovation (Source: pcaobus.org) (Source: pcaobus.org).
- SOX/ICFR Implications:** CFOs remain legally responsible for maintaining effective ICFR under SOX. Recent expert analyses emphasize that AI systems influencing financial data become part of the [SOX control environment](https://www.ridgewayfs.com). If AI “influences numbers, estimates, journal entries, reconciliations, or disclosures, it becomes part of your ICFR” (Source: www.ridgewayfs.com). Auditors will expect that any use of AI in financial processes be governed with controls analogous to other IT systems: access controls, change management, model validation, monitoring, and documented oversight (Source: www.ridgewayfs.com). High-risk uses of AI include automated postings to the general ledger or generation of key estimates; best practice is to retain “human-in-the-loop” controls with clear override logs and governance processes (Source: www.ridgewayfs.com).

- AI Adoption in Finance:** CFO attitudes toward AI are mixed but generally positive. Recent surveys show a majority of large-company CFOs view AI as strategically important. For example, in late-2025 only about 11–15% of CFOs had fully implemented AI in finance, but roughly 60–80% planned to adopt AI for at least some functions (Source: www.lek.com) (Source: www.deloitte.com). CFOs cite efficiency and data-analysis gains from AI, but also worry about systems integration and control challenges (Source: www.deloitte.com) (Source: www.lek.com). Industry commentaries emphasize that CFOs must assume an active governance role over AI: ensuring auditability, data accuracy, bias detection, and ethical use (Source: insightfulcfo.blog) (Source: insightfulcfo.blog). Internal guidance frameworks (e.g. COSO's GenAI roadmap, April 2026) now translate classic ICFR principles into GenAI-specific controls – highlighting that AI's probabilistic outputs must still be managed under rigorous internal control and monitoring (Source: www.prnewswire.com) (Source: internalaudit360.com).
- NetSuite and AI:** NetSuite (a widely-used cloud ERP system) has rapidly [embedded AI features](#) as of 2024–2025, including [generative text assistance](#) for data entry, AI-driven pricing/configuration helpers, and chat-based support agents (Source: www.prnewswire.com) (Source: www.prnewswire.com). CFOs and NetSuite administrators must understand that these AI-driven workflows intersect with SOX controls. For example, an [AI agent](#) that configures product prices or writes financial text must produce audit trails and be subject to supervisory review. NetSuite admins should configure and monitor AI features carefully (e.g. logging AI suggestions, enforcing approval workflows, protecting [prompt data](#) to ensure data integrity and compliance with ICFR requirements. As Deloitte research shows, CFOs overwhelmingly prefer AI capabilities **embedded** in trusted finance platforms, which implies that Oracle/NetSuite will likely continue integrating AI heavily (Source: www.lek.com). But this also means finance leaders must adapt their control frameworks to cover AI-assisted processes in their ERP.
- Regulatory Alignment and Global Context:** Domestic and international audit authorities are increasingly aligning on the promise and risks of AI. The PCAOB's U.S. policy reflects an "innovation-friendly but evidence-focused" approach: it encourages careful experimentation while clarifying that responsibility for sufficient evidence and audit quality still rests with auditors (Source: pcaobus.org) (Source: www.frc.org.uk). Notably, on March 30, 2026 the UK's Financial Reporting Council (FRC) issued its own guidance for audit firms on generative AI, explicitly stating that "the professional judgement and accountability of the auditor remains" central even as firms accelerate AI adoption (Source: www.frc.org.uk). COSO's April 2026 GenAI guidance similarly stresses that AI does not change the need for well-designed control environments, but rather requires "renewed rigor, clarity, and traceability" in applying established control principles (Source: www.prnewswire.com) (Source: www.prnewswire.com).

Recommendations for CFOs and NetSuite Admins: CFOs and finance teams should proactively incorporate AI into their ICFR risk assessments. This includes updating process documentation to cover AI-related steps, validating AI tools before use, and ensuring internal audit and external auditors have visibility into AI processes. NetSuite admins should inventory the suite's AI features, enforce secure configurations, and coordinate with finance/IT risk groups on testing and monitoring. Both sets of stakeholders should engage early with auditors around any AI integration: as PCAOB officials note, providing transparency about how data are used and trusting the auditors in a "co-pilot" role will be essential to maintain confidence and compliance (Source: pcaobus.org) (Source: www.frc.org.uk).

Below is a comprehensive analysis of these issues, combining detailed regulatory background, survey data, expert commentary, and illustrative examples. All claims are supported by citation to PCAOB releases, industry surveys, technical guidance documents, and other credible sources.

Introduction

The Sarbanes–Oxley Act of 2002 (SOX) mandates that public companies in the U.S. maintain effective internal control over financial reporting (ICFR). Under Section 404 of SOX, management must certify the design and operating effectiveness of ICFR, and their independent auditors must attest to that assessment. The **Public Company Accounting Oversight Board (PCAOB)** was created by SOX to oversee auditing firms and promulgate standards for public company audits (Source: en.wikipedia.org). In fulfilling its mandate—overseeing "informative, accurate, and independent" audits (Source: en.wikipedia.org)—the PCAOB must consider how emerging technologies like artificial intelligence affect the reliability of audit processes and financial reporting.

In recent years, **AI and machine learning (ML)** technologies have become pervasive across businesses and finance functions. Finance departments are using predictive analytics and even **generative AI (GenAI)** to automate routine tasks such as data entry, report drafting, forecasting, and anomaly detection. Many back-office processes are now partly or wholly AI-assisted – for example, using natural language generation to create narrative disclosures or chatbots to answer queries from accounting staff. ERP systems like Oracle NetSuite have embedded AI modules for automated text suggestions, product configuration assistants, and intelligent search (see "AI in NetSuite" below) (Source: www.prnewswire.com) (Source: www.prnewswire.com). External auditors are likewise investing in AI-driven audit tools: the Big Four now frequently describe their audit methodologies as "AI-first," with proprietary platforms (e.g. KPMG Clara, PwC's NextGen Audit platform) that use AI for data analytics, risk scoring, contract analysis, and even natural-language transcription of interviews (Source: kpmg.com) (Source: www.pwc.com).

This rapid AI adoption raises critical questions for the financial reporting ecosystem. From a CFO's standpoint, both the management and auditor sides of SOX compliance are implicated. If a company employs AI to produce or process financial data, then that AI is effectively an **element of the company's controls environment**, and any weaknesses could undermine ICFR. CFOs must therefore ensure that AI-driven processes have adequate oversight and auditability. Meanwhile, auditors face the challenge of integrating these new technologies into their audit procedures without compromising evidence quality. The PCAOB and other regulators are grappling with how existing standards apply when AI tools generate data or perform audit tasks.

This report explores the **PCAOB's stance on AI** in the context of SOX/ICFR audits as of 2026, and analyzes **implications for CFOs and NetSuite administrators**. It provides historical context, reviews PCAOB standards and guidance developments, surveys CFO and audit industry perspectives, and considers case examples. In doing so, it addresses questions such as: What guidance has the PCAOB given on auditors' use of AI? How should management think about AI in internal controls? How do CFOs view AI adoption, and what do they need to do operationally? And finally, how do cutting-edge AI features in NetSuite and other financial software intersect with SOX compliance? By synthesizing regulatory commentary, accounting research, and practitioner insight, this report aims to inform finance executives and system administrators about leveraging AI while maintaining SOX/ICFR integrity.

PCAOB and Auditing: Historical Context and Technology

PCAOB Overview

The PCAOB was established by the Sarbanes–Oxley Act of 2002 to oversee the audits of U.S. public companies (Source: en.wikipedia.org). Its mission is to protect investors by setting auditing standards and conducting inspections of registered audit firms to ensure high-quality, independent audit reports (Source: en.wikipedia.org). PCAOB standards (referred to as Auditing Standards, or AS) cover topics from risk assessment to substantive testing to reporting. For example, AS 2201 prescribes how auditors must audit management's assessment of ICFR (often referred to as AS 5 in earlier versions) when conducting an audit of financial statements.

Historically, PCAOB standards have been **technology-neutral** in that they did not prescribe specific technologies for auditors or issuers to use. For many years, auditors performed most work manually or with simple IT support, and PCAOB did not mandate the use of advanced analytics or AI. However, even a decade ago the PCAOB acknowledged that information technology was integral to audits: in 2012 the PCAOB adopted AS 2201 which, among other things, requires auditors to obtain an understanding of IT functions and controls that support ICFR. The PCAOB has issued staff guidance emphasizing that auditors must consider IT general controls and application controls when relying on electronic information (Source: pcaobus.org) (Source: pcaobus.org).

As data volumes and analytic capabilities have surged, the PCAOB's oversight naturally expanded in scope. In 2018 the PCAOB launched a **Data and Technology Initiative** to determine whether existing standards adequately cover new audit technologies. In October 2020, it published a "Study on the Use of Technology in the Audit of Financial Statements" (part of the Data & Tech project) assessing trends like data analytics and continuous auditing. That study recognized that "technology innovations ... can lead to improved audit quality but also create new audit risks" (e.g. data integrity, model risk). It encouraged auditors to adopt analytics but underpinned that with auditor responsibility for evidence (Source: pcaobus.org) (Source: www.deloitte.com).

Technology-Assisted Analysis: Recent PCAOB Standards Update

On June 12, 2024, the PCAOB adopted amendments to clarify auditors' responsibilities when using **technology-assisted analysis** (TAA) (Source: pcaobus.org). These amendments specifically updated AS 1105 ("Audit Evidence") and AS 2301 ("The Auditor's Responses to the Risks of Material Misstatement") to address procedures that use computers and algorithms to analyze electronic information. Key points of the 2024 amendments include:

- Emphasizing that auditors must evaluate the **reliability of electronic information** used as evidence: if an auditor tests controls over electronic information, the testing should include relevant IT general controls and automated application controls (Source: pcaobus.org). For example, if an AI model or software generates trial balance data, the auditor must consider the underlying IT controls that produced that data (Source: pcaobus.org).
- Clarifying that evidence obtained by technology (such as full-population analytics) can serve multiple purposes in the audit, but the auditor must ensure it meets the standard for sufficient appropriate evidence (Source: pcaobus.org). In other words, deriving audit conclusions through an AI-assisted process does not relieve the auditor of their obligation to obtain high-quality evidence consistent with AS 1105.

- Reinforcing that auditors remain responsible for designing and supervising procedures, even when using automated tools (Source: pcaobus.org) (Source: pcaobus.org). The adopting release explicitly states that adding detail around TAA is intended to reduce the risk that an audit opinion is issued without obtaining “sufficient appropriate audit evidence.” Notably, PCAOB Chair Erica Williams said the amendments would “help two essential standards keep pace with changes in the use of technology” and encourage the use of analytics (Source: pcaobus.org).

These amendments take effect for audits of fiscal years beginning on or after December 15, 2025 (Source: pcaobus.org). Thus for calendar-year 2026 audits, all issuers and their auditors must comply. CFOs should note that auditors will now more explicitly audit the IT environment and data reliability. In practice, this means firms may incorporate IT General Controls (ITGC) and controls over AI models into their ICFR testing, and will document how their analytics programs (including any AI components) were validated and supervised. The PCAOB’s emphasis is on **transparency and sufficiency of evidence**, not on barring the use of technology; indeed, the Board commented that the changes “should address some auditors’ reluctance ... to use technology-assisted analysis” under prior ambiguous standards (Source: pcaobus.org).

Citing these Standards. PCAOB’s own summary for auditors states: “Since AS 1105 and AS 2301 were issued in 2010, advancements in technology have enabled auditors to expand the use of technology-assisted analysis. The amendments are designed to decrease the likelihood that an auditor who performs audit procedures using technology-assisted analysis will issue an audit report without obtaining sufficient appropriate audit evidence” (Source: pcaobus.org). This encapsulates the PCAOB stance: it **encourages AI and data analytics use to strengthen audit quality**, but insists that auditors maintain their traditional responsibilities (e.g. understanding IT systems, evaluating data reliability, and judging results) when doing so.

PCAOB’s Recent Activity on AI and Technology

Technology Innovation Alliance (TIA) Working Group Recommendations

In November 2022, the PCAOB announced a *Technology Innovation Alliance (TIA) Working Group* to advise on emerging technologies’ impact on audits. The goal was for external technologists and audit professionals to recommend how the PCAOB might adapt its oversight and standards. The TIA, chaired by PCAOB Board Member Christina Ho, issued two major deliverables:

- **Current State Deliverable (Aug 30, 2023):** A study summarizing the audit profession’s present use of technology and attitudes toward it. It noted broad trends (e.g., high demand for tech-savvy auditors) and the sensitivity of audit quality to data and model risks.
- **Future State Deliverable (May 30, 2024):** Until recently kept internal, this set forth **four “strategic pillars”** for PCAOB direction. The report (publicly released by the PCAOB on Sep. 3, 2025 (Source: pcaobus.org) advocated: (1) *Standardized Audit Documentation* – create structured data in audit working papers to enable AI discovery and continuous auditing. (2) *Using AI in Audit* – A framework or guidance for responsible AI use by auditors, lowering perceived barriers to adoption. (3) *Regulatory Innovation Lab* – an audit-tech innovation sandbox to pilot standards and share learning before formal rule-making. (4) *Auditor Tech Literacy* – encourage training and curricula in data analytics and AI for auditors (Source: pcaobus.org).

These recommendations reflect a broad consensus that AI can materially improve audit quality if done correctly. The TIA report explicitly phrases innovation as an “engine that improves audit quality” and urges the PCAOB to play a leadership role in enabling safe adoption of AI (Source: pcaobus.org). CFOs and tech leads should note that the PCAOB is now thinking in terms of *promoting* AI (with guardrails), not simply regulating against misuse.

PCAOB Leadership Speeches

In September 2025, PCAOB Board Member Christina Ho (former chair of the TIA working group) delivered a major speech titled “AI and the Pursuit of Audit Quality: A Regulatory Perspective.” She outlined the TIA’s four pillars and explicitly called for PCAOB to “take a newfound leadership role” in driving innovation (Source: pcaobus.org). Key points from her remarks:

- She described technology-neutral standards as an **“anchor”** that can inadvertently hold back progress when tech changes rapidly (Source: pcaobus.org). Instead, she argued for agile, iterative approaches to standard-setting tailored for tech (seeing AI as requiring a more dynamic regulatory response) (Source: pcaobus.org) (Source: pcaobus.org).
- She gave a hypothetical example: if an audit firm tested *100% of journal entries* using an AI tool instead of traditional sampling, auditors might *actually* improve coverage. But without clear guidance, PCAOB inspectors might react by demanding extensive detail on the AI model (requiring the firm to “turn over every rock”). This could discourage the firm from using the AI test and revert to slower manual sampling, paradoxically

reducing quality (Source: pcaobus.org). The moral drawn was that PCAOB should aim to be an *engine* for innovation rather than an *anchor* holding it back (Source: pcaobus.org) (Source: pcaobus.org).

- She highlighted the second TIA pillar (“Using AI in Audit”) calling for risk management guidance and principles to help firms use AI responsibly (Source: pcaobus.org). Regulatory clarity, she said, incentivizes auditors to “leverage technology effectively” which ultimately “promote[s] audit quality” (Source: pcaobus.org).
- She announced (with reference) a co-authored paper recommending an “**agile standard-setting**” process: iterative sprints, pilot phases, and continuous stakeholder involvement rather than lengthy notice-and-comment alone (Source: pcaobus.org).

Member Ho concluded by stressing that while the profession is pushing ahead with AI, the PCAOB must “emerge out of the shadows” and issue the timely guidance needed to help auditors adopt AI and improve audit quality (Source: pcaobus.org).

Relevance: While these remarks reflect the views of one PCAOB member (not an official rule), they signal the Board’s direction of travel. The speech underscores that the PCAOB is seriously considering how to nurture AI usage rather than obstruct it. In practice, this could mean forthcoming staff guidance or updated inspection focus on AI risks and good practices. CFOs should anticipate that in future PCAOB inspections, auditors will be evaluated on how they supervise AI processes and maintain evidence, not just on whether they use sample tests or AI.

PCAOB Staff Outreach on Generative AI

On July 22, 2024, the PCAOB published a **Staff Spotlight** on Generative AI (GenAI) in audits (Source: pcaobus.org). In this outreach brief, PCAOB staff reported on discussions with major audit firms and corporate preparers about GenAI’s integration into audit and reporting. Notable observations included:

- Current usage of GenAI by audit firms was “limited but evolving quickly.” It was mostly applied to *administrative and research activities* (e.g. drafting work papers, looking up authoritative sources) (Source: pcaobus.org). However, firms expected GenAI could potentially be used in planning or substantive procedures in the future.
- Firms are investing in GenAI tools, but also **acknowledge limitations**. They stressed the need for strong supervision of GenAI use to guard against risks like data privacy and the known unpredictability of GenAI outputs (Source: pcaobus.org).
- Among corporate preparers (management), interest in GenAI was high across the business, but relatively *less* focus was on core accounting and financial reporting processes at that stage. In other words, while GenAI was broadly used in operations and front-office areas, few organizations had deeply integrated GenAI into accounting processes yet (Source: pcaobus.org).
- Importantly, PCAOB staff noted that they had reached out to most global networks and large firms auditing the majority of market cap, and were actively continuing to monitor developments in GenAI usage by all audit firms (Source: pcaobus.org).

This Spotlight report underscores that as of mid-2024, neither auditors nor companies had widely unleashed GenAI in SOX work, but everyone recognized the potential and was moving cautiously. For CFOs, the takeaway is that regulators are *aware* of AI use and expect companies to be forthcoming about it. The PCAOB explicitly **invited firms to share their experiences with GenAI** (Source: pcaobus.org), signaling that they will evaluate disclosures around AI risk. CFOs should ensure that any AI pilots or tools used in finance have enough documentation and monitoring that could be shared with auditors or regulators if asked.

Other PCAOB Activities

The PCAOB continues to maintain its Data and Technology project page, which includes staff reports and resources (Source: pcaobus.org). It also operates advisory groups, and in January 2026 announced members of its Standards and Emerging Issues Advisory Group (SEIAG) and Investor Advisory Group (Source: pcaobus.org). While those groups’ public charters may not specifically mention AI, advisory members often include technology experts whose input can shape future standard initiatives.

Overall, the PCAOB’s stance can be summarized as **procuring controlled adoption**: it is not imposing an outright ban or strict prohibitions on AI tools, but neither is it giving free rein. Instead, it is **clarifying auditor obligations** (via amended standards), **conducting outreach** (to gauge needs and concerns), and **encouraging dialogue** on best practices (via working groups and speeches). The Board has acknowledged auditors’ dual focus: they want to use data analytics and AI to improve coverage, but regulators want to ensure such use does not inadvertently cause evidence gaps or uncontrollable model risks.

AI and SOX/ICFR: Risk Management and Control Considerations

As CFOs integrate AI into financial processes, key questions arise: *Does AI change the rules of Sarbanes–Oxley?* Legally, it does not. Regardless of how data are generated or processed, a public company’s management is still required to maintain **effective ICFR** (as defined by COSO or similar frameworks) (Source: www.prnewswire.com) (Source: www.prnewswire.com), and include any relevant automated processes in its control matrix. Auditors, in turn, must test those controls and obtain sufficient evidence for their opinion.

However, AI does introduce **new layers of risk** into ICFR:

- **Opacity and Explainability:** Many AI/ML models, especially complex neural networks, are “black boxes” to end users. A CFO may not fully understand how an algorithm arrives at a forecast or classification. This opacity makes it hard to verify that the model is functioning correctly. COSO notes that GenAI’s “opaque reasoning” and frequent reconfiguration could jeopardize reporting integrity (Source: www.coso.org). Auditors will expect organizations to address this by either using interpretable models or implementing compensating controls for “explainability.”
- **Data Quality and Bias:** AI outputs are only as good as their inputs. If the input data to an AI system are incomplete, stale, or biased, the results (forecasts, working paper summaries, etc.) can be materially wrong. CFOs must ensure robust data governance. For example, if an AI system is used for revenue forecasting, the historical sales data feeding it must be validated and cleansed. Auditors may challenge blind faith in AI predictions; they will likely review data lineage and error rates.
- **Reliance and Human Oversight:** An excessive hands-off approach is risky. If auditors or management simply accept AI outputs without scrutiny, important anomalies may be missed. The consensus advice from internal audit and risk professionals is to maintain **human-in-the-loop** controls. As one advisory note states: “The safest approach is ‘human-in-the-loop’ controls with clear thresholds, logged overrides, and a documented model governance process” (Source: www.ridgewayfs.com). In practice, this means any AI-generated estimate or journal suggestion should be reviewed by a knowledgeable person, not just accepted automatically. CFOs should document who reviews AI outputs and what tolerances (e.g. variance thresholds) are used to trigger intervention.
- **Cybersecurity and Privacy:** AI systems often require data aggregation and, for generative AI, may involve sending data to cloud-based LLMs. There is a risk of sensitive financial or personal information exposure. Controls must ensure, for example, that prompts sent to an AI agent strip identifying information or use on-premises models. If auditors see evidence of unsecured data flows or improper handling of personal data, it would count as a control deficiency.
- **Change Management:** AI systems evolve over time, especially if they continuously learn or receive updates. Without proper change management, new versions of an algorithm could behave unpredictably. PCAOB’s amended AS 2301 emphasizes that change management for automated controls is an auditor responsibility (Source: pcaobus.org). CFOs should treat model tunings like any major IT change: approvals, testing, and documentation.

These AI-specific risks must be embedded into the existing ICFR framework (such as COSO’s five interrelated components: control environment, risk assessment, control activities, information/communication, monitoring) (Source: www.prnewswire.com) (Source: www.prnewswire.com). Fortunately, COSO’s *April 2026* guidance translates each COSO component into GenAI-specific practices. For example, under *Control Activities* it might suggest verifying that AI decision rules are reviewed by risk management, and under *Monitoring Activities* it includes auditing AI outputs for drift over time (Source: internalaudit360.com) (Source: www.prnewswire.com). CFOs should obtain and review the COSO GenAI report, as it offers many concrete checklists for AI governance (e.g. templates for AI risk inventories, control testing procedures, metrics) (Source: internalaudit360.com).

PCAOB Expectations for Auditors vs. Management

It is important to distinguish responsibilities. PCAOB and auditors regulate the **audit process**; they do not directly regulate management’s adoption of AI per se. However, auditors must respond to how management uses AI. The Ridgeway Financial analysis succinctly states: “*If AI influences [financial reporting], it becomes part of your ICFR*” (Source: www.ridgewayfs.com). This means management (including the CFO) must identify AI’s role in each key financial process and design controls around it (e.g. model validation, segregation of duties over AI operations). Auditors then verify those controls and perform testing that may include examining the AI models and outputs.

On the audit side, PCAOB clearly retains the principle that auditors are accountable for the audit opinion, regardless of how technologically sophisticated the audit approach becomes. For instance, the UK FRC guidance (adopted March 2026) emphasizes: “Firms and Responsible Individuals should note that regulatory accountability for deployment of AI tools and the quality of audit outputs remains unchanged. As set out in

auditing standards, the human auditor is always accountable” (Source: www.frc.org.uk). Similarly, PCAOB’s approach is that AI is a tool, but the auditor must use professional skepticism and judgement. The Deloitte discussion of an “auditor’s mindset in an AI-driven world” likewise stresses that auditors must evaluate AI governance and risks just as they would any other critical process (Source: www.deloitte.com) (Source: www.deloitte.com).

In summary: **CFOs own ICFR including AI components**, and must ensure controls and disclosures are updated accordingly. **Auditors must ensure they obtain sufficient evidence despite AI, and adapt their methods.** The PCAOB’s stance is collaborative rather than adversarial; inspectors have noted that firms are beginning to test larger data sets and use AI, and want clarity on acceptable practices. The amendments to AS 1105/2301 indicate inspectors will now specifically look for evidence of IT and AI control testing (Source: pcaobus.org) (Source: www.ridgewayfs.com). CFOs should thus be prepared to discuss with auditors any material AI usage (e.g. during walkthroughs) and demonstrate how such tools are governed.

AI in the Corporate Finance Function

CFO Survey Evidence on AI Adoption

Industry surveys reveal that FP&A and finance departments are actively exploring AI, though widespread deployment is still emerging. Deloitte’s 2025 “CFO Survey” (Brazil) found that **74% of CFOs plan to adopt GenAI for financial activities**, with 15% already doing so (Source: www.deloitte.com). The survey highlights that CFOs see AI as equivalent to higher efficiency: for example, 80% expect to use GenAI for routine tasks, 60% for planning/analysis, and 48% for transactional services (Source: www.deloitte.com). The primary concerns are pragmatic: 54% worry about integrating AI with existing financial systems, and 51% worry about training staff to use AI (Source: www.deloitte.com).

A separate 2025 L.E.K. Consulting survey of global CFOs reports similar findings (Source: www.lek.com). About 60% of CFOs agree that AI will be one of the most impactful technologies in finance, but only about 11% have fully deployed it in-house (Source: www.lek.com). Another 35% are experimenting with pilots. Interestingly, 25% already use AI-powered features within their finance software (e.g. predictive forecasting modules), and an additional 44% plan to do so within 3–5 years (Source: www.lek.com). Importantly, a clear majority of CFOs (56%) **prefer AI functionality built into their existing finance platforms** (like their ERP or accounting system), versus 31% who want best-of-breed standalone applications (Source: www.lek.com). This trend favors NetSuite-like embedded solutions. CFOs who have adopted AI report gains in productivity and quality, especially in accounts payable/receivable automation (Source: www.lek.com).

Key takeaway: CFOs broadly accept that AI is the future of finance, but most are still in early stages. They will lean on vendors’ built-in AI (e.g. NetSuite) rather than awkward bolt-ons. For the CFO audience, this means it’s timely to plan for AI’s impact on internally controlled processes. Even if adoption is partial today, survey data implies that finance teams will have much more AI-driven data by 2026–27.

Risk Management Principles for Finance

The arrival of AI prompts reinvigoration of internal control frameworks:

- **COSO Framework Alignment:** The COSO Internal Control – Integrated Framework (ICIF) remains the authoritative model for U.S. public companies to design ICFR. The new COSO GenAI guidance reaffirms this: it does *not* replace COSO’s five components, but augments them with AI-specific practices (Source: www.prnewswire.com) (Source: www.prnewswire.com). CFOs should map the AI elements in their processes onto the COSO cube: for example, under *Control Environment*, consider whether the audit committee understands AI risks; under *Control Activities*, ensure that model review is codified; under *Monitoring*, set up an AI performance dashboard.
- **Bias and Ethical Oversight:** CFOs must watch for biases inadvertently coded into financial decision tools. As one expert writes: “Bias in AI is not always nefarious – but it is always consequential,” possibly perpetuating historic inequities in supplier payments or credit assumptions (Source: insightfulcfo.blog). For example, a generative AI drafting management discussion might underrepresent uncertainties present in emerging markets, skewing investor expectations. Digitally auditing biases (by scenario testing or fairness checks) should be part of the finance group’s review. In effect, CFOs assume in their custody-of-trust role a mandate to “govern AI with integrity” and ensure systems are “accurate, explainable, [and] auditable” (Source: insightfulcfo.blog).
- **CFO ‘Flight Simulator’ Concept:** Some finance leaders liken AI governance to the simulation of an airplane’s behavior. You would never let autopilot fly without thoroughly testing it; similarly, CFOs should simulate AI outputs and stress-test them. For instance, run “GPT hallucination” tests: ask a language model edge-case questions and compare to known answers. Document such test results to show due diligence.

- **Audit Trail and Documentation:** With AI potentially generating outputs, CFOs should ensure outputs remain traceable. If NetSuite's CPQ AI recommends a product bundle, that advice should be logged. If a chatbot writes a variance explanation, that text should be tied back to its prompt and the model version. The goal is to maintain as good or better an audit trail than manual processes. Indeed, the Ridgeway guidance specifically calls for "evidence of review" for AI outputs (Source: www.ridgewayfs.com), implying records of who reviewed what and when.
- **Training and Change Management:** CFO teams should update job descriptions and training to include "AI oversight." Without competency among users, AI can turn into a black box used carelessly. COSO's Fourth Pillar (Encourage Technology Literacy) suggests budgeting for AI training in accounting curricula (Source: pcaobus.org). Internally, run periodic refresher training on both the technical and ethical aspects of AI usage.

Auditing Perspective: AI as an Audit Tool

Auditors are also rapidly integrating AI into their work. All of the Big Four firms have invested in audit platforms powered by data science or generative interfaces (Source: kpmg.com) (Source: www.pwc.com). For example:

- **KPMG** has developed *Audit Chat*, a generative AI assistant, and other GenAI tools (voice transcription, contract analyser). In a 2024 press release, KPMG reported 600,000 user "conversations" with its audit Chatbot within six months, aiding in risk assessments and research (Source: kpmg.com). KPMG emphasizes that these tools are "human-centric" – each AI capability is integrated with auditor judgement and aligned to professional standards (Source: kpmg.com).
- **PwC** markets a "Next Generation Audit" suite that applies predictive analytics and machine learning to enable earlier risk identification, deeper benchmarking and automated anomaly detection (Source: www.pwc.com). They tout that "AI and emerging tech have unlocked new possibilities" for enhanced audit quality.
- **Deloitte** has published thought leadership on auditors' role in AI governance. For instance, Deloitte's article "*An auditor's mindset in an AI-driven world*" notes that as organizations scale AI, auditors can leverage their risk assessment and controls expertise to promote trust and transparency (Source: www.deloitte.com) (Source: www.deloitte.com). The article explicitly states that auditors will work with management's "three lines of defense" to oversee AI – management owns first-line development, risk functions provide frameworks second-line, and internal audit forms the third-line review (Source: www.deloitte.com) (Source: www.deloitte.com).
- **IAASB / AICPA / Other Standards Bodies:** Global bodies are also active. For example, in March 2026 the UK's audit regulator (FRC) issued the first ever regulator guidance on *Generative and Agentic AI in audits* (Source: www.frc.org.uk). The guidance provides audit firms with a conceptual framework to gain appropriate confidence in AI outputs, and includes illustrative examples (e.g. using AI to summarize board minutes or analyze contracts) (Source: www.frc.org.uk). Critically, the FRC guidance reinforces that "while technology changes, the fundamental principle of our regulatory framework does not: it is people... who are accountable for audit quality" (Source: www.frc.org.uk). This aligns with PCAOB's stance that AI tools do not replace auditor judgement.

In sum, auditors are **embracing AI** as a way to perform more comprehensive examinations (e.g. testing 100% of data instead of samples), but they are conscious that this shift must be accompanied by guidelines. PCAOB's tech amendments and outreach essentially mirror this sentiment: they encourage the efficiency and depth AI offers (e.g. full-population analytics) but insist on rigorous evidence and understanding. The early emphasis is on data analytics and GenAI for "lookups and analysis," not on having AI sign off on opinions (Source: pcaobus.org).

From the CFO's perspective, the result is likely positive: audits may become more data-driven and arguably more reliable if firms correctly use AI. For example, anomalies not caught by judgmental sampling may be flagged by algorithmic scans. However, CFOs should be prepared for auditors to ask more questions about the IT/AI environment than before. Management will need to explain AI models to auditors: what inputs they use, how they were validated, what parameters are crucial, etc. Building that understanding now can smooth SOX audits later.

NetSuite and AI: Controls in Practice

NetSuite, as a leading cloud ERP, has been aggressive in adding AI features that affect finance operations. In early 2025 **Oracle NetSuite** announced five major generative AI capabilities for customers (Source: www.prnewswire.com). These include:

- **Text Enhance for Custom Fields:** Uses GenAI to suggest or auto-populate custom text fields in NetSuite forms (e.g. descriptions or notes) based on the company's historical data. Administrators can configure prompts through a "Prompt Studio" to tailor tone and format (Source: www.prnewswire.com).

- **Prompt Management API:** A centralized interface for managing AI prompts and model calls. This allows SuiteCloud developers and integrators to build custom SuiteApps that invoke Large Language Models, with control over prompt behavior (Source: www.prnewswire.com).
- **NetSuite CPQ AI Assistant:** An AI chat agent to assist with Configure-Price-Quote processes. Salespeople can converse with the agent to find product configurations; the agent recommends bundle options based on a natural language dialog (Source: www.prnewswire.com).
- **NetSuite Expert for SuiteAnswers:** An AI-powered help assistant. Users ask natural-language questions about NetSuite processes, and the agent searches across the support knowledge base to provide answers and guidance (Source: www.prnewswire.com).

For NetSuite **administrators**, these new tools mean more configuration and control points:

- **Data Quality:** With Text Enhance, AI may insert text based on any existing data. Admins should verify that default suggestions (e.g. from historical order descriptions) remain accurate and current. If NetSuite's training data include outdated or misclassified entries, the AI might perpetuate errors. Therefore, it may be wise to periodically sample AI-generated field entries and compare to actual outcomes, adjusting filters or blacklists as needed.
- **Access Controls:** The Prompt Management API essentially delegates AI capabilities to SuiteApps. Admins must secure these APIs: ensure only approved scripts can call AI models, and that the data sent to the AI (prompts) do not contain confidential fields. Logging prompt usage (user, time, prompt content) will help in audits if questions arise about AI outputs.
- **Audit Trail of Approvals:** AI-generated suggestions (e.g. automated journal descriptions or CPQ recommendations) should ideally not bypass existing approval workflows. For instance, if Text Enhance populates a journal memo, the usual process for authorizing that entry should still apply. Any time the AI fills or edits a field, that change should be tracked in the system's history with the user ID who accepted or modified it. This ensures an audit trail.
- **Explainability:** Since NetSuite's AI features are generative, admins should document how decisions are made. For highly material processes (like revenue recognition calculations suggested by AI), NetSuite may offer logs of AI sessions. If not, companies might need to record prompts and responses manually. Having a policy that high-risk AI outputs must include a "reasoning" or justification can make later reviews easier.
- **Human-in-the-Loop:** The Ridgeway ICFR guidance advises "human-in-the-loop" with overrides and clear thresholds (Source: www.ridgewayfs.com). NetSuite workflows can enforce this. For example, a policy could state that any AI-suggested journal entry exceeding a certain amount requires manual check. Or a QA step could be added that a finance team lead reviews a random sample of AI-populated fields each week.
- **Vendor & Version Control:** NetSuite's AI features may update frequently (since they integrate external LLMs). Admins should allocate responsibility for monitoring release notes, testing new versions (especially since generative models can change behavior with updates), and aligning them with SOX change management.

In practice, **NetSuite Admins and finance teams should collaborate**. Admins can set up AI in the system, but CFOs/staff need policies on how to use it. This cross-functional team should include internal audit or IT risk so that AI usage is visible in the audit of NetSuite environment.

NetSuite's Position: Notably, NetSuite is positioning these AI tools as cost-free enhancements ("embedded AI at the core of the suite... at no additional cost" (Source: www.prnewswire.com). This reduces a CFO's excuse to delay testing them – since they're part of the platform you already pay for. But the same Oracle PR also hints: "prompt-based manipulation" is a risk (Source: www.coso.org). In other words, giving the wrong prompts could produce misleading data, and CFOs should be cautious about what prompts are used or stored (especially if they might inadvertently expose strategy or forecasts to the AI).

Controls and NetSuite: Example Table

The table below summarizes a few of NetSuite's new AI features and the high-level control considerations for each:

NETSUITE AI FEATURE	DESCRIPTION	SOX/CONTROL IMPLICATIONS
Text Enhance for Custom Fields (Source: www.prnewswire.com)	Auto-generates text suggestions for free-text fields (e.g. journals, memos) using company data.	<i>Control Data Quality:</i> Regularly review samples of AI-suggested text for accuracy. <i>Approval Workflow:</i> Ensure AI-populated fields still go through approval. <i>Logging:</i> Track which entries were AI-generated vs. manually entered.
Prompt Management API (Source: www.prnewswire.com)	Central API to manage and customize prompts for LLM integrations in SuiteApps.	<i>Access Control:</i> Restrict who can use or call the API. <i>Prompt Review:</i> Audit prompt templates to avoid leaking sensitive info. <i>Change Mgmt:</i> Treat prompt updates as configuration changes needing review.
CPQ AI Assistant (Source: www.prnewswire.com)	AI chatbot that recommends product/service configurations via natural language querying.	<i>Calculation Controls:</i> Review AI-proposed config for correct pricing, discounts, tax. <i>Audit Trail:</i> Log the conversation and final config selected. <i>Override Authority:</i> Only authorized sales/support can finalize an AI suggestion.
NetSuite Expert (SuiteAnswers) (Source: www.prnewswire.com)	AI agent that answers how-to questions using NetSuite's knowledge base.	<i>Content Control:</i> Validate the guidance the AI gives (since it may hallucinate). <i>Access:</i> Limit advanced troubleshooting via AI to trained staff. <i>Audit:</i> Note any material decisions (e.g. how to handle an exception) that relied on AI advice.

(The control implications above are illustrative; CFOs and NetSuite admins should adapt based on company risk profile. The **Ridgeway ICFR guide** and **COSO GenAI framework** can be consulted for more granular control strategies (Source: www.ridgewayfs.com) (Source: www.prnewswire.com.)

Case Studies and Examples

While comprehensive academic studies on AI in audit are still emerging, several real-world illustrations and pilot projects shed light on what CFOs can expect.

- **AI-driven Fraud Detection:** Some companies are piloting anomaly-detection algorithms on transaction data (a form of unsupervised ML). For example, MindBridge Ai offers an audit intelligence platform that uses machine learning to score and rank transaction anomalies (Source: pcaobus.org). Auditors can plug a general ledger into these tools to flag suspicious entries. CFOs considering similar internal tools should ensure they integrate with controls (e.g. flagged items trigger exception reporting and investigation steps).
- **ChatGPT for Financial Analysis:** A CFO might experiment with generative AI (e.g. ChatGPT or a finance-specific LLM) to auto-generate monthly financial commentary or risk assessments. A case reported an internal audit department (Uniper) using ChatGPT to streamline audit documentation (Source: www.ivysci.com). They stressed that such AI use required careful oversight: the audit team structured prompts to ensure completeness, and auditors still verified all outputs. Key lesson: generative text can reduce grunt work, but output must be checked.
- **Audit Sampling vs. 100% Testing:** The hypothetical statistician scenario from Christina Ho's PCAOB speech (testing 100% of journals by AI vs. sampling) highlights a potential. In practice, EY or PwC might already offer "Continuous Client Audit" services that tie into ERP systems, where AI or data analytics continuously screen transactions. If a CFO's NetSuite can share data, auditors could move toward more continuous models. But for any firm doing so, the auditors will likely audit the analytics process itself: they may request details of the AI model, its training, and its performance. CFOs should be prepared to produce this under inspection if they adopt such approaches.
- **Municipal or Global Differences:** Multinational CFOs should note that foreign regulators are also active. In Europe, audit regulators and standard-setters have been studying AI's impact. For instance, the International Auditing and Assurance Standards Board (IAASB) launched a technology focus area. While not directly affecting U.S. PCAOB standards, these initiatives signal that global trends move in the same direction.
- **Misuse Example (Hypothetical):** Consider a scenario (not a reported case but illustrative): a company uses an AI model to estimate bad-debt reserves, feeding it historical write-offs. If the model has an error or bias (e.g., is overweighting a booming historical period), the reserve will be wrong. If that AI model was treated as a "black box" and management simply signed off on its output, the company could face an SEC

restatement for misstated reserves. An auditor is trained to be skeptical and would likely test the reserve calculation by recalculating it or analyzing its assumptions. Hence management must ensure the AI model's assumptions and adjustments (if any) are documented for auditors to review.

These examples reinforce that **transparency and review are paramount**. CFOs may cooperate with auditors to pilot AI tools, but should do so with explicit test plans and controls validated by internal audit before results become final.

Implications and Future Directions

Auditor-Client Collaboration

Given the rapid pace of change, CFOs should see auditors as *collaborators* in innovation. As PCAOB Member Ho noted, regulators desire clarity to avoid a scenario where firms “go back to manual sampling because it’s less risky from a PCAOB compliance standpoint” (Source: pcaobus.org). To prevent that, CFOs and auditors should discuss early: if management plans to adopt an AI tool for a finance function, share prototypes or data flows with the audit team. Perhaps auditors can agree on joint validation of the AI output. This mutual planning echoes the call for an “Innovation Lab” in auditing, albeit informally at first.

Standard-Setting Outlook

The TIA Report and Christina Ho’s speech suggest new PCAOB standards or guidance may be forthcoming. CFOs should monitor the PCAOB website and professional accounting news for updates to AS 2201 (ICFR audit standard) or new practice alerts. For example, PCAOB could issue a **Staff Audit Practice Alert** on auditing AI outputs, akin to past alerts on IT or fraud. Given the PCAOB’s intense focus on tech, something like this is plausible.

Ongoing Regulatory Developments

- **COSO GenAI Guidance (April 2026):** Already released, it provides a practical internal control roadmap for GenAI use (Source: www.prnewswire.com) (Source: www.prnewswire.com). CFOs should integrate its recommendations into their risk assessment (e.g. using COSO’s “capability taxonomy” of AI use cases and controls). Moreover, Deloitte’s DART summary (April 3, 2026) of the COSO guidance highlights that “GenAI risk is an internal control challenge, not a policy discussion” (Source: rsmus.com).
- **SEC and Other US Agencies:** The SEC itself is building in-house AI capacity and has an AI Task Force (2025) but has not yet issued SOX-specific AI rules. However, CFOs should note that already the SEC requires in IFRS (management) representations to disclose any significant changes to internal control, which could be interpreted to include significant AI changes. State or federal initiatives on AI (e.g. NIST AI standards) may eventually influence auditing norms.
- **Audit Firm Initiatives:** Expect audit firms to standardize their own AI tools further. The big firms may require clients to use certain platforms (“provide your data to our AI tooling”) or may roll out new services like “AI audit of internal control.” CFOs should engage with their auditors to understand what software/platforms will be used in their audits, and what data/information needs to be provided to support that.

NetSuite and Vendor Roadmaps

For NetSuite users, it is likely that Oracle will continue to add AI-driven features. Already, the February 2025 news (see above) was one of many planned enhancements. Oracle may also start offering AI governance features (for example, MDM layer logging, or sandbox testing for AI configurations). CFOs and admins should seek Oracle’s security and compliance documentation on these AI features. It may become standard for cloud ERP vendors to include statements on auditability of AI modules.

Training and Professional Development

Finally, CFOs should invest in team education. Section 404 audits now may include questions about AI, and unfamiliarity is no excuse. Encouraging CFOs and controllers to attend AI-risk seminars or even CPE courses on data analytics will pay dividends. NetSuite Admins should likewise get training (NetSuite offers free learning paths on AI) (Source: docs.oracle.com). The PCAOB’s fourth strategic pillar (promoting tech literacy) anticipates this need (Source: pcaobus.org).

In sum, 2026 represents a **transition year**. Early adopters have tested the waters; regulators have signaled strong interest. CFOs who proactively upgrade their SOX work to include AI considerations will be ahead of the curve. Those who do not may face audit questions or even control findings (if, say, auditors report a deficiency that “AI model governance was insufficient”). By aligning with the principles expressed by both PCAOB and

oversight bodies, finance leaders can turn AI into an asset rather than a liability for compliance and decision-making.

Conclusion

Artificial intelligence is poised to transform finance and auditing. For CFOs and NetSuite administrators, the message is clear: **you cannot ignore AI or pretend it isn't part of your controls environment**. The PCAOB has made preliminary moves to clarify how auditors should handle technology-assisted audit work, and regulators around the world are codifying guidance to manage AI risk. At the same time, market forces are pushing technology into the fold: CFO surveys and ERP vendor roadmaps show that AI incorporation is accelerating.

Therefore, a proactive approach is needed. CFOs should chart an AI strategy that balances innovation with diligence: adopt AI for efficiency and insight, **but** build robust controls, documentation, and training around it. NetSuite and similar systems will continue to release AI-driven functionality; savvy finance teams will leverage these features while insisting on audit trails, override controls, and ongoing monitoring.

On the audit side, the PCAOB's stance can be summarized as: *"Use AI to enhance audit quality, but don't skip the fundamentals."* This means expecting more sophisticated evidence-gathering (like data analytics) under the amended standards (Source: pcaobus.org), but also auditing that these technologies are reliable. It also means communicating with your auditors about any AI tools in your financial processes, so they are aware and can assess related risks. As one PCAOB official put it, the board wants auditors to **"perform high-quality audits using technology-assisted analysis"** (Source: pcaobus.org) – a call that implicitly extends to auditors scrutinizing the AI usage of their clients.

Finally, the outlook is clear: AI will only grow in importance. Future regulatory work is likely to **encourage** AI in audits (through guidance and possibly new standards) and **expect discipline** in its application to financial reporting. If CFOs and NetSuite admins stay informed and forward-looking, they will not only comply with SOX requirements, but potentially derive competitive advantage through smarter, AI-enabled finance operations. The journey will involve trial and error, but by grounding AI deployment in the principles of internal control and audit evidence, the finance organization can safely venture into this new frontier.

References

All references are provided inline above in [source+L...] notation, corresponding to the URLs and document line numbers from the PCAOB, COSO, Deloitte, KPMG, Oracle NetSuite, academic, and news sources cited. The PCAOB website and press releases were primary sources for regulatory updates (Source: pcaobus.org) (Source: pcaobus.org). Industry surveys (Deloitte, L.E.K.) and professional commentary (COSO, Ridgeway Financial, Deloitte, etc.) provided practitioner perspectives (Source: www.deloitte.com) (Source: www.lek.com) (Source: insightfulcfo.blog) (Source: www.ridgewayfs.com). Where applicable, global regulatory guidance (FRC Generative AI guidance) and academic articles were also cited (Source: www.frc.org.uk) (Source: www.deloitte.com). Each quoted or paraphrased claim above is backed by one or more of these authoritative sources.

Tags: pcaob ai standards, sox compliance, icfr audits, netsuite ai, ai internal controls, coso genai framework, financial reporting, audit technology

DISCLAIMER

This document is provided for informational purposes only. No representations or warranties are made regarding the accuracy, completeness, or reliability of its contents. Any use of this information is at your own risk. Houseblend shall not be liable for any damages arising from the use of this document. This content may include material generated with assistance from artificial intelligence tools, which may contain errors or inaccuracies. Readers should verify critical information independently. All product names, trademarks, and registered trademarks mentioned are property of their respective owners and are used for identification purposes only. Use of these names does not imply endorsement. This document does not constitute professional or legal advice. For specific guidance related to your needs, please consult qualified professionals.