Managing Sarbanes-Oxley in a Transforming Landscape: A Case Study

Kaden E. Salazar

Colorado State University

Week 1 Case Study Assignment 1

CIS 563: Information Assurance and Security

Dr. Charles Butler

August 29, 2025

Case Study Managing Sarbanes-Oxley in a Transforming Landscape

Sarbanes-Oxley Act (SOX) is a policy put in place in 2002 after numerous large business committed accounting fraud, including Enron (SEC, 2003) and WorldCom (WorldCom, 2004), to create more transparent accounting practices and ultimately protect shareholders (H.R.3763, 2002). Section 404 of SOX may be one of the most referenced sections, as this section lays the foundation of what a company is required to do to meet its reporting criteria. Section 404(a) requires management to assess how effective internal controls are in regard to financial reporting, and Section 404(b) requires an auditor to attest to management assessment of the previously mentioned controls (H.R.3763, 2002). Essentially, this is what holds companies accountable for their accounting practice, but it comes with many hurdles for companies seeking compliance, and with the ever shifting 404 landscape, companies may find themselves lagging behind.

Key Issues

Critical Audit Matters (CAMs)

With SOX also came the Public Company Accounting Oversight Board (PCAOB), as outlined in Section 101 of SOX act. In 2017, PCAOB created a new auding standard, AS 3101, which defined Critical Audit Matters (CAMs) as any issue arising from an audit that is both material to the financial statements and involved especially challenging, subjective, or complex auditor judgment (PCAOB, 2017). Since 2020, all public companies have been subject to this requirement. While CAM disclosures were intended to provide transparency to investors, they also highlight areas where controls may be vulnerable. Deficiencies tied to judgment-heavy processes, such as revenue recognition or impairment testing, can influence the determination of a CAM. Although terms like “significant deficiency” are not directly used in the disclosure, the underlying control weaknesses may still be revealed indirectly, raising reputational and compliance risks for organizations.

PCAOB Auditing Standard 2501

Accounting estimates represent another significant challenge for SOX compliance. These estimates, such as allowance for loan losses, valuation of financial instruments, goodwill impairments, and inventory reserves, rely heavily on management judgment. In 2019, PCAOB issued Auditing Standard 2501 to strengthen auditor evaluation of these estimates. The standard requires auditors not only to understand management’s methodology but also to develop their own independent expectation, supported by reasonable assumptions and reliable data (PCAOB, 2019a).

In particular an amendment to paragraph .12 of AS 2501 connects directly to AS 1105 by requiring auditors, when relying on company-produced information, to perform

procedures that test the accuracy and completeness of the information, or test the controls over that accuracy and completeness, including IT general controls and automated application controls, and evaluate whether the information is sufficiently precise and detailed for purposes of the audit.

This amendment has important implications for organizations. First, it raises the standard for internal controls around data that supports estimates. Information used to calculate reserves, impairments, or fair values must be demonstrably complete, accurate, and detailed, not just directionally correct. Second, it places added emphasis on IT general controls and automated application controls. If an organization's systems feed data into financial reporting processes, those systems must have strong, documented controls that auditors can test. Finally, it reduces management's ability to rely on broad or high-level assumptions without rigorous supporting evidence. Any weaknesses in how information is gathered, validated, or controlled could now undermine both the estimate and the overall audit opinion.

Cyber risk and controls

Although cybersecurity is not explicitly covered under SOX, it has become a central concern due to its impact on financial reporting and safeguarding of assets (Exabeam, 2025). Organizations rely more than ever on automated systems, cloud platforms, and robotic process automation (RPA) to perform financial functions. These technologies increase efficiency but also introduce vulnerabilities (Eulerich et al., 2023). Phishing scams and wire transfer fraud, for example, have caused substantial financial losses for companies, raising questions about whether controls are robust enough to prevent or detect such events. Similarly, if a hacker were to compromise bots used for financial close or SOX testing, the integrity of reporting could be manipulated. Because of these risks, auditors are increasingly inquiring into companies' cyber-risk profiles. Controls over disbursements, cash transfers, and system access are now scrutinized as indirect components of SOX compliance, perhaps even more so now after the previously mentioned amendment to AS 2501, making cybersecurity integration into internal control frameworks an unavoidable issue.

Shifting PCAOB focus

In addition to addressing specific audit standards, the PCAOB has broadened its oversight to firm-wide methodologies, training, and quality controls. Its 2019 concept release signaled potential revisions to quality control standards, which could significantly reshape how audit firms operate (PCAOB, 2019b). This shift has cascading effects on public companies because changes in audit methodology often translate into higher

expectations for management's controls and documentation. Companies that fail to anticipate these evolving expectations may face longer audits, increased costs, or higher risk of identified deficiencies. The trend highlights that SOX compliance is not static and rather is influenced not only by legislative mandates but also by the regulatory bodies that enforce and interpret them. For organizations, the challenge is to remain adaptable as the PCAOB pushes auditors toward greater rigor and consistency in their practices.

Discussion

SOX remains critically important today as the bedrock of investor confidence and fraud deterrence. By enforcing rigorous internal controls and financial reporting standards, SOX strengthens transparency and holds executives personally accountable. In practice, SOX compliance has expanded into information security as. So, SOX is not just a legal formality but a proactive safeguard that boosts investor trust and corporate resilience

SOX has also adapted to new risks. Modern compliance goes well beyond checking boxes and it must now embrace technology and emerging threats. For instance, SOX programs now routinely involve IT and cybersecurity experts as firms leverage AI, cloud systems, and robotic automation in finance (IMB, 2023). Industry leaders urge that cybersecurity and data-privacy assessments be integrated into SOX risk management. In this evolving landscape, SOX compliance must be forward.

With these dynamics in mind, we compare two broad approaches for each key issue:

Critical Audit Matters:

Option 1, management reacts to CAMs only when auditors raise them, implementing only basic disclosure controls. This reactive stance risks surprises late in the audit; undisclosed control weaknesses in judgment-heavy areas may emerge only at year-end, possibly triggering material adjustments or negative auditor commentary. Option 2, management engages auditors early to identify likely CAM topics and stress-tests related controls. For example, Protiviti consultants recommend that internal audit should talk to their auditors to identify any items that will lead to CAMs and then fortify those controls in advance (Audit Board, 2024). This second approach helps surface and fix issues before they become CAMs, reducing audit friction and reputational risk. Auditors then know where to focus, and management can prevent control gaps from becoming public disclosures

Accounting Estimates and Complex Valuations:

Option 1, management assumes existing estimation controls suffice. Under PCAOB AS 2501, however, auditors now develop their own independent expectations of estimates, so if management's controls are outdated, auditors may find inconsistencies or biases late

in the process. Option 2, companies tighten estimate controls by ensuring the underlying data is accurate and assumptions are well-documented. This means reconciling data sources, documenting how key assumptions were chosen, and even stress-testing alternative outcomes. By improving data governance and independently validating inputs, management can satisfy auditors' expectations and avoid disputes over assumptions.

Cybersecurity and Emerging IT Risks:

Option 1, management addresses cyber threats with a separate IT security program, assuming SOX covers only financial processes. The danger here is as auditors probe financial systems, any cyber breach or unauthorized bot activity affecting the closing process can undermine the audit. For example, if an RPA bot used in the financial close is compromised or untracked, auditors may later flag that as an internal control deficiency. Option 2, companies integrate Cyber into SOX Controls. This means including IT general controls. In practice, integrating cyber into SOX encourages using shared controls, for example, IAM systems that enforce segregation of duties support both IT security and SOX compliance (IBM, 2023). This holistic approach reduces gaps between the IT department and finance, whereas isolating them as in option 1 might leave financial reporting exposed to undetected hacks or fraud.

Shifting PCAOB Focus and Audit Standards:

Option 1, management waits for auditors to implement new PCAOB requirements and only then adjusts documentation or controls. This reactive stance can mean higher costs or delays when standards change. If management remains passive, it may face longer audits or more findings. Option 2, proactive companies monitor PCAOB/SEC updates, adopt leading practices, and continuously train their teams. Engaging with industry groups, sharing experiences, and rehearsing new audit processes can smooth the transition. Option 2 means viewing SOX as a dynamic program rather than a static set of checklists.

Recommendations

Meet with your external auditors well before year-end to surface potential Critical Audit Matters (CAMs) and difficult audit issues. By identifying likely CAMs in advance, management can strengthen related controls and disclosures. Protiviti advises internal audit to ask auditors about items that "will lead to CAMs" and then bolster the underlying controls (Audit Board, 2024). In practice, this means drafting preliminary CAM descriptions, testing those areas proactively, and clarifying judgment points early. This early dialogue reduces surprises and aligns expectations, turning CAMs from red flags into opportunities to demonstrate robust controls.

Tighten estimate controls with precision and independent checks. Enhance the rigor around accounting estimates by improving data quality and validation. Ensure that the data feeding your reserves, impairments, and fair-value models are complete, up-to-date, and reconciled to source systems. Document all key assumptions (and changes to them) with evidence from market or operational data. Where possible, use third-party benchmarks or industry indices to challenge management's estimates. Even internal data models should be stress-tested: for example, model the estimate under alternative scenarios to check sensitivity. By incorporating independent expectation-setting and robust IT controls into the estimation process, in line with AS 2501 guidance, management can give auditors confidence that the numbers are reasonable and reduce the likelihood of last-minute adjustments.

Integrate cybersecurity and IT controls into SOX risk assessments. Treat cyber threats as financial-reporting risks, not separate issues. Include IT general controls (e.g. user access, change management) and automated application controls in the inventory of key SOX controls. As the industry guidance notes, integrate cybersecurity and data privacy into the SOX framework (Cross Country Consulting, 2025). This may involve partnering with IT to define what constitutes a "material" breach for your business and ensuring rapid reporting if such an incident occurs. Using technology tools, like SIEM for event logging, automated access reviews, and secure documentation systems, they protect systems and simultaneously generate potential SOX audit evidence. Training finance and IT teams together on internal control objectives can also help everyone understand how cyber incidents could affect financial reporting.

Likely one of the most important recommendations that can be given is to stay informed. Maintain ongoing dialogue with regulators, auditors, and peers. Assigning a team or individual to track PCAOB standards and SEC rulemaking and participating in industry forums or workgroups to share best practices could prove valuable. Given the PCAOB's shift toward risk-based audit quality standards (PCAOB, 2019b), consider conducting mock inspections or internal audits against emerging criteria. Document your governance updates and train the control owners regularly. In essence, build a compliance culture that is audit ready year-round, not just at year-end. This might mean annual control self-assessments, scenario-based risk workshops, or cross-functional steering committees to adapt SOX processes as business and technology evolve.

References

Audit Board. (2024, September 20). *Critical Audit Matters (CAMs): What You Need To Know*. Auditboard.com. https://auditboard.com/blog/critical-audit-matters-what-you-need-to-know

Cross Country Consulting. (2025, July 17). *SOX Modernization & Optimization Strategy Roadmap 2025-2026*. CrossCountry Consulting. https://www.crosscountry-consulting.com/insights/blog/strategies-for-sox-program-optimization-and-modernization/

Eulerich, M., Waddoups, N., Wagener, M., & Wood, D. A. (2023). The Dark Side of Robotic Process Automation (RPA): Understanding Risks and Challenges with RPA. *Accounting Horizons*, *38*(2), 1–10. https://doi.org/10.2308/horizons-2022-019

Exabeam. (2025, February 18). SOX Cybersecurity Requirements and Best Practices for 2025. Exabeam. https://www.exabeam.com/explainers/sox-compliance/sox-cybersecurity-requirements-and-best-practices/

H.R.3763 - 107th Congress (2001-2002): Sarbanes-Oxley Act of 2002. (2002, July 30). https://www.congress.gov/bill/107th-congress/house-bill/3763

IBM. (2023, October 19). *SOX compliance*. Ibm.com; IBM. https://www.ibm.com/think/topics/sox-compliance

PCAOB. (2017). *AS 3101: The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion*. https://pcaobus.org/oversight/standards/auditing-standards/details/AS3101

PCAOB. (2019a). *AS 2501: Auditing Accounting Estimates, Including Fair Value Measurements*. https://pcaobus.org/oversight/standards/auditing-standards/details/AS2501

PCAOB. (2019b). *Concept Release Potential Approach to Revisions to PCAOB Quality Control Standards*. https://pcaobus.org/Rulemaking/Docket046/2019-003-Quality-Control-Concept-Release.pdf

SEC. (2003, March 17). *SEC Charges Merrill Lynch, Four Merrill Lynch Executives with Aiding and Abetting Enron Accounting Fraud*. Sec.gov. https://www.sec.gov/news/press/2003-32.htm

WorldCom, Inc. (2004 March 12). Form 10-K for the fiscal year ended December 31, 2002. SEC EDGAR,

https://www.sec.gov/Archives/edgar/data/723527/000119312504039709/d10k.htm#tx43272_19