MODERNIZING THE SARBANES-OXLEY ACT

PROTECTING CAPITAL MARKETS, STRENGTHENING INVESTOR PROTECTIONS, & REDUCING COMPLIANCE COSTS

An IIA Public Policy Position Paper

The Institute of Internal Auditors

Contents

Executive Summary

The purpose of this paper is to serve as a reference document as U.S. lawmakers and their staff provide on-going oversight and consider the future evolution of the Sarbanes-Oxley Act (SOX) and its implementation.

For over two decades, SOX has been a cornerstone of the corporate governance and investor protection legal and regulatory framework underpinning U.S. capital markets. By establishing defined responsibilities for governing bodies, executive management, and external auditors, the law has strengthened financial reporting integrity and enhanced investor confidence.

However, as organizations increasingly adopt advanced technologies – such as automation, artificial intelligence, quantum computing, and continuous data monitoring – policymakers will need to ensure that SOX evolves to remain relevant and effective in today's rapidly changing economic and regulatory environment.

Since its passage, several policymakers have sought to monitor the efficiency and effectiveness of the law in reaching its goals. More recently, there have been a few significant congressional activities which have put the law back into the policy spotlight. In particular, there was an unsuccessful effort, in early 2025, to dissolve the Public Company Accounting Oversight Board (PCAOB) and fold its responsibilities into the Securities and Exchange Commission (SEC) and, on June 25, 2025, the U.S. House Financial Services Subcommittee on Capital Markets held a hearing regarding the cost of SOX compliance.

These activities indicate a potential enhanced interest by some Members of Congress in revisiting the law. While SOX does not explicitly recognize the role of internal audit, the PCAOB has acknowledged the profession's place within the broader compliance and assurance ecosystem.[1] The Institute of Internal Auditors (The IIA) believes this is an important step, but Congress and the PCAOB can do more to strengthen organizational assurance by more fully integrating internal audit into SOX compliance.

In light of recent congressional actions, should a SOX legislative window of opportunity occur, The IIA seeks, through this paper, to proactively provide Congress and relevant federal regulators with its recommendations on how SOX and its implementation might be improved, specifically as it relates to SOX's relationship to the internal audit profession.

The IIA's principal recommendations are:

1) **Enhance legal and regulatory clarity**, codifying the definitions of "internal auditing" and the "internal audit function" and formally articulating the internal audit profession's

[1] The Public Company Accounting Oversight Board specifically outlines the role of internal audit in certain SOX compliance activities in the following auditing standards: AS 2201, *An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements*; and, AS 2605, *Consideration of the Internal Audit Function*.

standards, roles, and responsibilities in providing assurance to governing bodies and executive management, and partnering with external financial auditors to support SOX compliance.

2) **Re-examine contemporary understandings of compliance in relation to Sections 302 and 404 of SOX**, with a particular focus on the role of internal audit functions in meeting those compliance requirements.

3) **Better establish internal and external auditors as partners in the assurance ecosystem**, enhancing collaboration and coordination between the two.

4) **Explore opportunities for SOX compliance cost reductions**, with a focus on how emerging technologies and enhanced collaboration with internal audit functions may advance those goals.

5) **Ask federal regulators to engage more fully with the internal audit profession**, ensuring that internal auditors "have a seat at the table" and that regulators are educating stakeholders about the value of the internal audit function in regards to SOX and protecting investors and capital markets.

At a time when Congress considers weighing both the effectiveness and cost of SOX compliance, the recommendations outlined in this paper offer a practical path to strengthening investor protection while promoting efficiency and resilience in U.S. capital markets.

By more clearly recognizing and integrating the internal audit function within the SOX framework, policymakers can reinforce accountability, improve coordination across the assurance ecosystem, reduce duplication of effort and associated compliance costs, and better align the law with modern risk, technology, and governance realities. Such actions would not only preserve the core objectives of SOX, but also help ensure that its implementation remains fit for purpose in a rapidly evolving economic environment by supporting market confidence, regulatory effectiveness, and long-term economic growth.

For additional information and resources related to SOX or other topics, policymakers and their staff may contact The IIA's Advocacy team at advocacy@theiia.org.

Overview of the Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX) was enacted by Congress in 2002 following several catastrophic corporate governance failures – including Enron and WorldCom – that revealed deep deficiencies in internal controls, assurance, auditor independence, and board oversight. These scandals significantly undermined public trust in U.S. capital markets and prompted Congress to implement comprehensive reforms designed to strengthen financial reporting integrity, reinforce corporate accountability, and restore investor confidence.[2]

SOX introduced a new legal and regulatory framework that profoundly altered the existing governance and audit landscape. Among its most consequential provisions, the law established the Public Company Accounting Oversight Board (PCAOB) to provide independent oversight of the external audit profession and promulgate specific auditing and quality-control standards. It also required chief executive officers and chief financial officers to personally certify the accuracy and completeness of financial statements under Section 302, thereby heightening executive accountability for financial disclosures.

Moreover, Section 404 – arguably the centerpiece of SOX – mandates that management must annually assess the effectiveness of internal controls over financial reporting (ICFR). It further requires that external auditors, as part of an annual financial statement review, also provide an independent assessment regarding the effectiveness of an organization's ICFR. This requirement has fundamentally changed how organizations design, operate, and monitor their control environments.

The Role of Internal Audit in Supporting SOX Compliance

Given internal audit's unique role in providing an organization's governing body – and by extension management – with objective assurance and advisory services, the profession has long been essential in supporting an effective control environment, which is the foundation of SOX compliance. Internal auditors enhance organizational confidence in SOX-related disclosures by independently evaluating, among other things, that:

- Governance processes operate as intended
- Risks are properly identified and managed
- Internal controls are appropriately designed and operating effectively

Although SOX does not explicitly define or reference internal audit, the profession has indirectly served a critical role in contributing to many of the law's most significant provisions. For example, internal audit often provides on-going, independent assurance on the design and operating effectiveness of key internal controls. These insights provide the governing body and

[2] Peregrine, M. W., & Elson, C. W. (2022, August 30). *The Important Legacy of the Sarbanes-Oxley Act*. Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2022/08/30/the-important-legacy-of-the-sarbanes-oxley-act/

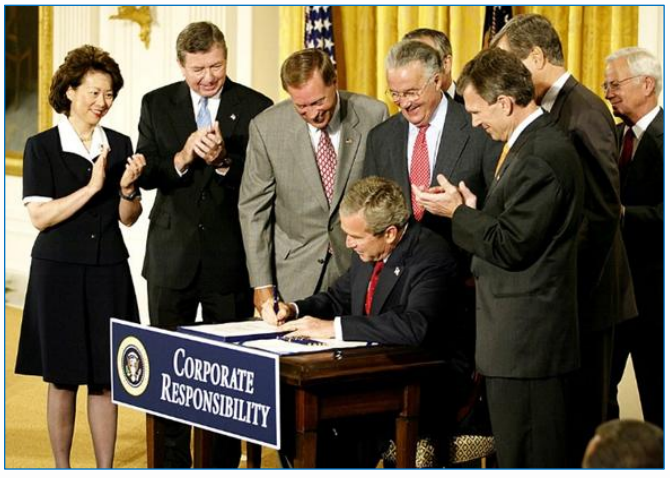
management with assurance that supports the assessments and certification obligations under Sections 302 and 404.

Through execution of their risk-based, independent internal audit plan, internal audit often helps organizations identify control deficiencies, validate risk-remediation efforts, and ensure consistent application of control standards across business units. When appropriately utilized by an organization to support Section 404 activities, the work of internal audit can also:

- Reduce the risk of material misstatements
- Strengthen compliance readiness for external audit testing
- Enhance the reliability of management's internal control assertions

In other words, internal audit leverages a deep understanding of the organization to conduct evaluations designed to promote transparency and accountability. This unique approach to oversight is important because it ensures the professionals performing assessments possess a thorough knowledge of the organization's strategic goals, culture, processes, and control environment. These powerful insights produce internal audits that provide a governing body with substantive and actionable information.

Despite these contributions, the SOX compliance environment faces structural challenges. After more than two decades, organizations continue to face fragmented interpretations of SOX requirements across regulators, auditors, and industries. Such a disjointed approach often leads to unnecessary duplication, inefficiency, and compliance costs that do not proportionately improve control quality.



U.S. President George W. Bush signs the "Sarbanes-Oxley Act of 2002" into law as members of the Congressional leadership and Cabinet watch in the East Room of the White House, 30 July 2002.
(STEPHEN JAFFE/AFP via Getty Images).

At the same time, the risk landscape has evolved dramatically. Digital transformation, automation, and increasingly complex cyber and data threats introduce new categories of risk that can affect financial reporting and internal controls. Maintaining SOX's effectiveness requires a modern, principles- and risk-based approach that leverages internal audit, aligns compliance with today's technology, and upholds transparency, accountability, and investor protection.

What Is Internal Auditing?[3]

Internal audit plays a vital role in promoting transparency, accountability, and trust across all sectors of the economy. Through independent assurance, an internal audit function supports both the governing body and management of an organization in achieving strategic and operational objectives. Its work strengthens organizational resilience by assessing the effectiveness of governance, risk management, and control processes.

Through systematic evaluation of risk, as well as the processes and key controls that mitigate it, internal auditors:

- Identify vulnerabilities that may impede performance or compliance
- Assess the adequacy of risk mitigation strategies
- Test the effectiveness of control processes
- Advise leadership on opportunities for improvement
- Help leaders proactively mitigate emerging risks

This combination of assurance and advisory support enables an organization's leadership to make informed decisions that strengthen performance and safeguard stakeholder interests. Moreover, the assurance and advisory role of internal audit extends beyond SOX compliance and financial reporting to encompass broader areas such as:

- Artificial intelligence
- Cybersecurity
- Data privacy
- Fraud prevention and detection
- Operational efficiency and organizational behavior
- Third-party risk management
- Other forms of legal and regulatory compliance

A key distinguishing feature of a properly structured internal audit function is its independence from management.[4] Internal auditors should functionally report to the organization's governing body, such as the board of directors or the board's audit committee.[5] This structural independence is a hallmark of the profession and is essential to maintaining objectivity, trust, and

[3] Since policymakers and their staff may have varying degrees of familiarity with internal auditing and its relationship to SOX, The IIA offers this overview of the profession to level set understanding for all stakeholders.

[4] The independence of a properly structured internal audit function is derived by conformity with The Institute of Internal Auditors' Global Internal Audit Standards™.

[5] Internal audit functions may, however, report to the CEO, CFO, or other relevant member of management for *administrative* purposes.

credibility. It also empowers internal auditors to identify and communicate organizational risks and challenges without fear of reprisal.

The essential elements of internal audit – independence, assurance, risk-based approach, and advisory services – define the profession's role in effective governance as follows:

- **Independence** – Grounded in integrity and accountability, internal audit provides an unbiased source of information to both governing bodies and senior management. True independence is derived from an internal audit charter which ensures appropriate organizational positioning – including functional reporting to the board or audit committee – authority over the internal audit budget; unrestricted access to information, people, and records; and the freedom to communicate results without interference.

- **Assurance** – Internal audit provides assurance that an organization's governance, risk management, and internal control processes are designed and operating effectively to achieve strategic, operational, financial, non-financial, and compliance objectives. This assurance provides the governing body with support on their oversight responsibilities and provides senior management with confidence that the organization's systems and processes are functioning as intended.

- **Risk-Based Approach** – Internal audit applies a risk-based approach, focusing its work on the areas of greatest risk to the achievement of organizational objectives. Audit priorities are informed by enterprise-wide risk assessments and evolving business, technology, and regulatory risks, allowing internal audit to provide timely assurance and advice where it matters most.

- **Advisory Services** – Beyond assurance, internal audit provides expert advisory services that provide a catalyst for continuous improvement in managing enterprise risks and enhancing the internal control environment. Through analysis, evaluation, and recommendations, internal auditors help enhance the efficiency and effectiveness of operations, identify emerging risks, and promote innovation in governance and risk management practices.

These responsibilities are embodied in The IIA's globally recognized professional principles known as the International Professional Practices Framework® (IPPF®). The IIA's IPPF provides the foundation for the success of the global internal audit profession. It ensures consistency, quality, and alignment across internal audit practices worldwide. The IPPF consists of three core elements:

- **Global Internal Audit Standards™ (Standards)** – The Standards guide the worldwide professional practice of internal auditing and serve as the basis for evaluating and elevating the quality of the internal audit function. The Standards are developed in the public interest through a due process conducted by the International Internal Audit Standards Board and overseen by the IPPF Oversight Council.

- **Topical Requirements** – These requirements are mandatory for assurance engagements and recommended for advisory work on pervasive global risk subjects when the topic identified during a risk assessment exceeds a significant risk level. Topical Requirements establish a consistent minimum baseline for coverage in designated risk areas. Internal auditors must apply additional procedures when organizational risks, regulations, or context demand greater depth.[6]

- **Global Guidance** – Referred to as Supplemental Guidance within the Standards, Global Guidance comprises Global Practice Guides and Global Technology Audit Guides®. These materials provide detailed directions for conducting internal audit activities and examples of deliverables. Sector-specific guides are also available for public sector audit and financial services internal audit functions.[7]

The IPPF and its components provide internal auditors with the methodologies, knowledge, and guidance necessary to perform their duties effectively and consistently across organizations and industries. The Standards require internal audit functions to undergo regular internal and external quality assurance assessments to evaluate compliance with professional standards. These assessments validate conformance, identify improvement opportunities, and reinforce the credibility of the internal audit activity. Therefore, adherence to these standards not only ensures high-quality audit work, but also reinforces the ethical and professional expectations of internal audit.

Building on this foundation of competence and integrity, internal auditors can further demonstrate mastery through professional certification. The only globally recognized certification for the profession is the **Certified Internal Auditor® (CIA®)** credential. The CIA represents the highest standard of professional achievement, reflecting expertise in the profession's core principles and practices.

Earning the CIA signifies not only technical proficiency, but also a commitment to integrity, continuous learning, and professional excellence. It enhances credibility, communicates expertise to employers and stakeholders, and underscores an internal auditor's ability to deliver value through sound judgment, strategic insight, and effective guidance in governance, risk management, and internal controls.

[6] The Institute of Internal Auditors. *Topical Requirements.* https://www.theiia.org/en/standards/2024-standards/topical-requirements/

[7] The Institute of Internal Auditors. *Global Guidance*. https://www.theiia.org/en/standards/2024-standards/global-guidance/

The Role of Internal Audit vs. External Audit

While both internal and external auditors play critical roles in ensuring the integrity of corporate and financial reporting, their responsibilities differ significantly in scope, timing, and focus. A clear understanding of these distinctions is essential for policymakers as they provide oversight of SOX and sound corporate governance public policy.

Overview of Internal Audit

As indicated above, internal audit functions operate as a continuous, proactive monitoring mechanism within an organization. Internal audit is one model that evaluates the design and effectiveness of operations and control processes, assesses emerging risks, and provides recommendations for improvement.

In accordance with Section 404 of SOX, management is required to assess and report on the effectiveness of internal controls over financial reporting (ICFR). Although internal audit is not specifically referenced in the law, the internal audit function can play an important supporting role in this process by conducting the required testing and validation of these controls necessary to validate management's opinion on the sufficiency of its ICFR under Section 404. With deep familiarity of organizational processes, and structured, reliable testing approaches, internal audit is uniquely positioned to identify weaknesses and propose remediation strategies, while helping management and the board of directors anticipate and mitigate future risks.

It is important to note that SOX compliance is supported by multiple layers of oversight, with second-line management functions also playing a key role in setting standards, monitoring control effectiveness, and guiding remediation efforts. While internal audit provides independent assurance, it is not the only mechanism for SOX compliance – management, risk, and compliance functions all contribute to sustaining an effective internal control environment. Together, these activities create a coordinated approach to meeting SOX requirements and maintaining reliable financial reporting.

In addition to compliance, internal audit also fosters a culture of accountability and on-going improvement. Through its advisory work, internal audit helps support sound governance, risk management, and control practices across the enterprise. These contributions not only support SOX compliance, but also enhance organizational resilience while protecting the public interest regarding operations beyond ICFR. [8]

[8] In addition to supporting compliance activities pursuant to Section 302 and 404, internal audit often plays a role in Section 301 of SOX which governs the treatment of whistleblower complaints related to "internal accounting controls, or auditing matters."

Overview of External Audit

In contrast to internal audit's continuous, risk-based, organization-wide focus, external audit engagements operate under specific statutory mandates. External auditors provide an independent evaluation of a company's financial statements.[9] Their primary objective is to determine whether an organization fairly presents its financial position in accordance with generally accepted accounting principles. Under Section 404 of SOX, external auditors must also attest to the effectiveness of the organization's ICFR at a single point in time, providing shareholders and regulators with independent assurance regarding the accuracy and reliability of management's assessments.

The scope of external audit is narrower than that of internal audit, focusing specifically on financial reporting and related internal controls. External auditors perform risk-based testing, concentrating on areas that could yield a potential material misstatement within the financial statements. Similar to internal auditors, their independence from management and direct reporting line to the board and/or its audit committee ensures objectivity and enhances the credibility of the organization's financial disclosures.

Complementary Roles and Coordination

While their roles and mandates are distinct, internal audit and external audit are integral components of a unified assurance ecosystem that support effective SOX compliance and investor protection. When appropriately coordinated, the two functions can reduce unnecessary duplication, improve audit efficiency, and lower overall compliance costs without compromising independence or rigor.

PCAOB Auditing Standard (AS) 2605, *Consideration of the Internal Audit Function*, recognizes that external auditors may use the work of internal auditors after evaluating competence, objectivity, and quality.[10] This framework is best understood not as establishing a hierarchy between the two functions, but acknowledging that internal audit's independently performed work creates value within the financial reporting assurance process. The ability of external auditors to rely on internal audit – where appropriate – allows organizations to derive greater benefit from assurance activities already being performed, rather than duplicating effort. In fact, a 2025 study released by KPMG revealed that, among those surveyed, "most respondents allocated over 60% of total internal audit hours to SOX compliance than two years ago."[11]

Internal audit and external audit are complementary assurance providers, each of whom are accountable to the organization's governing body and operating under distinct professional standards. External audit's mandate is focused on providing assurance over financial statements

[9] Gartner, Inc., *Definition of External Audit*, Gartner Finance Glossary. https://www.gartner.com/en/finance/glossary/external-audit

[10] Public Company Accounting Oversight Board. *AS 2605: Consideration of the Internal Audit Function*. https://pcaobus.org/oversight/standards/auditing-standards/details/as-2605-consideration-of-the-internal-audit-function_1528

[11] KPMG LLP. *The 2025 SOX Survey*. 2025. KPMG. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/the-2025-sox-survey.pdf

and ICFR, while internal audit conducts ongoing, risk-based evaluations across enterprise-wide governance, risk management, and internal control processes. This broader scope enables internal audit to provide continuous insight into emerging risks, control design, and operating effectiveness well beyond the boundaries of SOX.

Under Section 404, management is responsible for performing its own risk assessment to determine the processes and key controls in scope for ICFR testing. In addition, external auditors are also required to conduct an independent risk assessment in forming their audit opinion. Internal audit likewise maintains its own independent, enterprise-wide risk assessment, informed – but not driven – by the perspectives of management and the external auditor. Alignment among these assessments, while preserving their independence, is a critical driver of efficiency.

In practice, some of the most significant SOX cost savings arise when internal audit is structured with sufficient independence and rigor such that external auditors can evaluate and place appropriate reliance on the quality and reliability of internal audit's ICFR work. While external auditors must still perform required walkthroughs, design testing, and evaluation of higher-risk controls, greater reliance on high-quality internal audit work can meaningfully reduce duplicative testing and disruption to management.

Additional efficiencies are achieved when management, internal audit, and external audit align on ICFR scope, key processes, and control attributes early in the audit cycle. This alignment supports clear expectations, minimizes redundant requests, and allows each assurance provider to focus on its respective responsibilities while maximizing overall coverage.

This cooperative, reliance-enabled model reflects the modern role of internal audit as an independent, objective assurance function that enhances external audit. When internal and external audit operate as complementary pillars within the assurance ecosystem, organizations realize stronger governance, more efficient SOX compliance, and more effective protection for investors and other stakeholders.

IIA Recommendations for Enhancing SOX

Building on the observations already outlined in this paper – including the distinct yet complementary roles of internal and external audit, the challenges created by inconsistent reliance practices, and the absence of statutory recognition of internal audit – The IIA has identified several opportunities to strengthen SOX programs.

The following recommendations are designed to enhance clarity, modernize assurance expectations, promote investor protection, and ensure more efficient and effective oversight across organizations subject to the law.

1) **Enhance legal and regulatory clarity**, codifying the definitions of "internal auditing" and the "internal audit function" and formally articulating the internal audit profession's roles and responsibilities in partnering with governing bodies, executive management, external financial auditors, and other assurance providers to support SOX compliance.

   The absence of any direct reference to internal audit in SOX, as previously noted in this paper, creates regulatory ambiguity: Internal audit plays a vital role in an organization's risk management framework and can increase the efficiency and effectiveness of SOX activities, yet the law neither acknowledges nor defines the function. This statutory silence may lead to inconsistent expectations among governing bodies, uneven reliance by external auditors, and misalignment between corporate governance practices and regulatory oversight.

   To address this legal inconsistency, The IIA believes that any potential amendments to SOX should include definitions for both "internal auditing" and "internal audit function." Such modifications will establish clear and consistent considerations regarding successfully structured, properly supported, and independent internal audit functions.

   The IIA's Standards define internal auditing as:

   > *An independent, objective assurance and advisory service designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.*[12]

   Inclusion of this or a similar legal definition is essential because it would acknowledge, for the first time, the essential role internal audit performs in support of Sections 302 and 404 of SOX.

[12] The Institute of Internal Auditors. *Complete Global Internal Audit Standards.* https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/free-documents/complete-global-internal-audit-standards/

In defining an internal audit function, The IIA recommends that any legal definition include, at a minimum, the following essential criteria:

- Independence from management, with direct accountability to the governing body or its audit committee
- A written internal audit charter, approved by the governing body and the Chief Audit Executive (CAE)
- Adherence to the Global Internal Audit Standards
- Qualified staff that is demonstrated through work experience, and appropriate certifications or credentials – such as the CIA or relevant specialty designations
- The ability to operate objectively and without conflicts of interest
- An established quality assurance and improvement program which would include regular internal quality assessments coupled with external quality assessments at least once every five years

Characteristics of a Properly Structured Internal Audit Function

The IIA believes that a strong and clearly defined internal audit function is vital for enhancing governance, strengthening risk management, and helping organizations meet their legal and ethical obligations under SOX. By codifying these definitions and criteria, policymakers can promote consistency, professionalism, and effectiveness – ensuring that all stakeholders who utilize internal audit leverage the function to its maximum potential.

2) **Re-examine contemporary understandings of compliance in relation to Sections 302 and 404 of SOX**, with a particular focus on the role of internal audit functions in meeting those compliance requirements.

As indicated earlier, Section 302 of SOX requires the principal executive officers (Chief Executive Officer and Chief Financial Officer) of issuers to certify in their financial reports that: 1) they have reviewed the report, 2) they are unaware of any untrue statement or omission of material fact, and 3) the financial statement and other financial information fairly present the financial condition and results of operations of the issuer. Furthermore, the signing officers are responsible for:

- Establishing and maintaining internal controls
- Designing internal controls to ensure that they are made aware of all material information
- Evaluating the effectiveness of the issuer's internal controls within 90 days of the report
- Presenting in the report their conclusions about the effectiveness of their internal controls based on their evaluations as of that date

Finally, under this section, the signing officers must disclose to the external auditors and the audit committee of the board of directors all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data. They must also identify for the external auditors any fraud or material weakness in internal controls.

Since the law, itself, does not provide specific guidance over how officers can ensure they comply with the law, The IIA believes that all stakeholders – lawmakers, regulators, external auditors, and corporate officers – should be engaged in on-going and robust discussion about how to demonstrate compliance, which, of course, may evolve, over time, with the result being more sophisticated regulatory and shareholder expectations.

Because the internal audit function is designed to provide assurance over internal controls, The IIA believes it should be viewed as an essential component of investor protection.

Therefore, as all stakeholders continue to examine and revisit the concept of compliance with Section 302, The IIA suggests that the following questions merit careful debate and consideration:

- ***Can an issuer's internal controls be considered effective and in compliance with Section 302 absent the regular risk-based independent assurance supplied by an internal audit function?***
- ***Should an organization's principal executive financial officers be required to explain the processes utilized to provide assurances over controls in the absence of an independent internal audit function?***

- ***In complying with Section 302, for those issuers with internal audit functions, should the principal executive officers explain the steps they have taken to ensure that the internal audit function is independent, objective, and properly resourced and structured?***

While many stakeholders may find these questions to represent a significant departure from some earlier understandings of compliance, The IIA believes that their consideration is timely. Perspectives on compliance and market requirements are not static and should be treated as ever evolving in our dynamic economy.

In a similar manner, internal audit plays a critical supporting role in compliance with Section 404 by providing independent, objective assurance regarding the design and operating effectiveness of internal controls over financial reporting. Although management retains full responsibility for establishing, maintaining, and assessing internal controls, internal audit's risk-based evaluations, testing activities, and validation of remediation efforts can meaningfully inform management's assessment and strengthen the overall reliability of the internal control framework supporting financial reporting.

As perspectives on Section 404 compliance continue to evolve, The IIA believes it is appropriate for stakeholders to consider whether effective compliance can be demonstrated in the absence of regular, independent assurance over internal control effectiveness. For issuers with internal audit functions, additional consideration may be warranted as to whether management should explain how the independence, objectivity, and resourcing of internal audit contribute to the integrity of the Section 404 assessment process. These considerations are intended to promote greater transparency and confidence in the internal control environment, while preserving management's ultimate accountability under the statute.

Since these questions represent a new way of thinking about SOX compliance, The IIA is not calling for any specific actions by lawmakers or regulators in the short term. Rather, the organization prefers that all stakeholders have time for reflection, debate, and refinement of their views, with the possibility that legal and/or regulatory clarity may be warranted at a later date.

3) **Better establish internal and external auditors as partners in the assurance ecosystem**, enhancing collaboration and coordination between the two.

Given the absence of any explicit reference to internal auditing within SOX, there is an opportunity to strengthen regulatory coordination among the assurance functions that collectively support effective SOX compliance. Policymakers, regulators, external auditors, internal auditors, management, and governing bodies all have a role in advancing a more coordinated assurance ecosystem – one that recognizes internal and

external audit as independent, complementary providers of assurance acting in the interests of shareholders.

In this context, The IIA recommends an on-going role for the PCAOB in fostering effective collaboration and alignment. This may be accomplished by clarifying expectations for registered firms regarding how they engage with internal audit functions in a manner that preserves independence while enabling appropriate reliance. Such clarity can help organizations realize greater value from assurance activities already being performed, reduce unnecessary duplication, and lower the overall cost and burden of SOX compliance.

PCAOB leadership has acknowledged the important role of internal auditors, stating that "internal auditors can and often do play an important role in enhancing the quality of a company's financial reporting."[13] Consistent with this view, The IIA has invested in building sustained engagement with PCAOB leaders to reinforce the value of internal audit and to explore practical ways external auditors and internal auditors can work together more effectively within existing regulatory frameworks.

One concrete, near-term opportunity for the PCAOB to advance this objective is through targeted revisions to AS 2605, *Consideration of the Internal Audit Function*. AS 2605 provides guidance to external auditors on how to evaluate and use the work of internal audit in connection with financial statement audits and ICFR pursuant to SOX. The standard currently states:

> *If the auditor decides that it would be efficient to consider how the internal auditors' work might affect the nature, timing, and extent of audit procedures, the auditor should assess the competence and objectivity of the internal audit function in light of the intended effect of the internal auditors' work on the audit.*[14]

The IIA agrees that external auditors must perform appropriate due diligence when determining whether, and to what extent, they can rely on the work of internal audit. However, The IIA believes that assessments of internal audit's competence and objectivity under AS 2605 should be benchmarked against conformity with the IPPF. The IPPF provides a globally recognized basis for confidence in the quality, consistency, and reliability of internal audit work, reduces the risk of inconsistent or subjective evaluations, and supports more efficient reliance decisions.

Clarifying this expectation would not alter the external auditor's independent responsibilities or judgment, nor would it require reliance on internal audit work. Rather,

[13] "The Auditor's Use of Confirmation, and Other Amendments to PCAOB Standards," Public Company Accounting Oversight Board, September 28, 2023. https://assets.pcaobus.org/pcaob-dev/docs/default-source/rulemaking/docket_028/2023-008_confirmation-adopting-release.pdf?sfvrsn=e18cef74_4

[14] Public Company Accounting Oversight Board. *AS 2605: Consideration of the Internal Audit Function*. https://pcaobus.org/oversight/standards/auditing-standards/details/as-2605-consideration-of-the-internal-audit-function_1528

it would reinforce a regulatory framework in which high-quality, independent internal audit functions are positioned to contribute meaningfully to SOX assurance where appropriate by:

- Supporting audit efficiency
- Reducing duplicative testing
- Strengthening assurance, overall governance, and internal control environments

The IIA looks forward to continued engagement with the PCAOB and other stakeholders to advance a balanced, reliance-enabled model of cooperation between internal and external auditors that enhances investor protection and the resilience of U.S. capital markets.

4) **Explore opportunities for SOX compliance cost reductions**, with a focus on how emerging technologies and better collaboration with internal audit functions may advance those goals.

Since its enactment into law, several stakeholders have expressed concerns about the cost of SOX compliance. And, indeed, a recent report from the U.S. Government Accountability Office (GAO) highlights that the organizational cost of SOX compliance remains high. While absolute compliance costs are higher for larger companies, GAO noted that the relative burden is often more significant for smaller firms.[15] During a hearing of the U.S. House Subcommittee on Capital Markets on June 25, 2025, Mr. Lawrence Cunningham, Director of the Weinberg Center for Corporate Governance at the University of Delaware, relayed this finding, testifying:

> *The burden of SOX compliance – especially under Section 404(b) – is both heavy and growing. Direct costs are high and rising: building control systems, documenting them, testing them, and paying external auditors to attest to them. Indirect costs are harder to quantify – and likely higher still.*[16]

While several factors drive rising compliance costs, incorporating emerging technologies (e.g., artificial intelligence, continuous data monitoring, etc.) and strengthening collaboration between internal and external audit functions may offer practical ways to enhance efficiency and reduce expenses. Furthermore, The IIA's research on the cost of internal audit functions also indicates that they are a low-cost, high-value private sector solution for providing shareholders with assurance and policymakers should look to better leverage their value.[17]

---

[15] U.S. Government Accountability Office. (2025, June 18). *Sarbanes-Oxley Act: Compliance Costs Are Higher for Larger Companies but More Burdensome for Smaller Ones* (Report No. GAO-25-107500). https://www.gao.gov/products/gao-25-107500

[16] Cunningham, L. A. (2025, June 25). *Testimony before the Subcommittee on Capital Markets, U.S. House Committee on Financial Services*. https://docs.house.gov/meetings/BA/BA16/20250625/118419/HHRG-119-BA16-Wstate-CunninghamL-20250625.pdf

[17] For additional information on the cost of an internal audit function, see the Appendix.

The IIA believes that it is timely for Congress to hold additional hearings on this topic to help lawmakers and regulators better understand how the compliance environment has changed in the past two decades. It is prudent to identify new opportunities for protecting investors while addressing compliance costs. The IIA is prepared to serve as a resource to Congress, contributing its expertise in effective corporate governance to help explore practical, sustainable solutions.

5) **Ask federal regulators to engage more fully and consistently with the internal audit profession**, ensuring that internal auditors "have a seat at the table" and that regulators are educating stakeholders about the value of the internal audit function regarding SOX.

   Federal regulators can play an important role in enhancing the value of internal audit functions in SOX's implementation and the protection of shareholders.

   Recognizing these benefits, The IIA encourages federal regulators to take concrete steps to strengthen these relationships.

   In particular, The IIA is making two short-term recommendations.

   1) The IIA has requested that the SEC post online guidance describing the proper development and structure of internal audit functions within listed companies. Such a resource would help companies – especially those newly entering public markets and becoming subject to SOX – understand the importance of establishing effective internal control processes and building strong assurance capabilities. Clear recommendations from the SEC would promote consistency, strengthen governance and assurance arrangements, and support a sound baseline of internal audit quality across registrants.

   2) The IIA is requesting that the PCAOB prioritize ensuring there is representation from the internal audit profession on its Standards and Emerging Issues Advisory Group (SEIAG). Internal audit participation on the SEIAG would enrich the PCAOB's understanding of emerging risks, enhance the practical relevance of its standards, and promote better alignment across the broader assurance ecosystem. Moreover, internal auditors can provide real-time insight and advise on how proposed standards affect internal control frameworks, operational practices, and audit coordination within companies.

   In essence, The IIA believes that federal regulators cannot fully achieve their mission without understanding and engaging with the internal audit profession. Internal auditors can provide critical intelligence, act as a bridge between management and oversight bodies, and help ensure that regulatory objectives are met efficiently and effectively. Strengthening this relationship is not only beneficial – it is essential for protecting the public interest and safeguarding the integrity of U.S. capital markets.

Conclusion

More than 20 years after its enactment, the Sarbanes-Oxley Act remains a foundational pillar of U.S. corporate governance and investor protection. Its core objectives – enhancing accountability, strengthening internal controls, and preserving trust in capital markets – continue to be vital. At the same time, the business, risk, and technology environment in which SOX operates has evolved significantly, creating both challenges and opportunities for policymakers, regulators, and market participants.

As Congress and federal regulators evaluate the effectiveness, efficiency, and future direction of SOX, this position paper articulates how internal audit plays a critical – though largely unrecognized – role in supporting the law's objectives. Internal audit functions provide continuous, independent, and risk-based assurance that strengthens management's internal control assessments, enhances board oversight, and supports high-quality external audits. When appropriately structured and resourced, internal audit functions, with their reliability and quality safeguarded through adherence to globally recognized professional standards, contribute meaningfully to investor protection while helping organizations manage complexity, emerging risks, and compliance costs.

The recommendations outlined in this paper offer a pragmatic and forward-looking framework for potential SOX modernization while strongly supporting the law's fundamental purpose. By clarifying the legal and regulatory status of internal audit, re-examining contemporary interpretations of compliance, strengthening collaboration between internal and external auditors, and engaging more directly with the internal audit profession, policymakers can reinforce the effectiveness of SOX while promoting smarter, more resilient oversight and assurance.

These recommendations are designed to inform an on-going dialogue as Congress and regulators assess how SOX can remain fit for purpose in a rapidly evolving economy. Recognizing and better integrating internal audit within the SOX framework represents an opportunity to enhance assurance quality, reduce unnecessary duplication, and align compliance expectations with modern governance and risk management practices.

The Institute of Internal Auditors stands ready to serve as a resource to Congress, the SEC, the PCAOB, and other stakeholders as these policy discussions continue. By working collaboratively to strengthen the assurance ecosystem, policymakers can preserve the enduring strengths of SOX while ensuring that it continues to protect the public interest, support confidence in U.S. capital markets, and promote long-term economic growth.

Specific Requested Actions Within The IIA's Recommendations

CONGRESS

- Pass legislation to define "internal auditing" and the "internal audit function" and clarify internal audit functions' relationship and added value to external auditors in regard to SOX compliance.

- Hold hearings on SOX compliance costs and how emerging technologies, better coordination between internal and external auditors, and properly structured internal audit functions can protect investors while potentially reducing costs.

PCAOB

- Update the Auditing Standard, *Consideration of the Internal Audit Function* (AS 2605), so that evaluations of "competence and objectivity" of internal audit functions by external auditors are measured against one criterion: conformance with The IIA's International Professional Practices Framework.

- Prioritize inclusion of an internal audit profession representative on the PCAOB's Standards and Emerging Issues Advisory Group (SEIAG).

SEC

- Provide recommended guidance on the Commission's website as to how issuers can establish and maintain an independent, and properly resourced and structured, internal audit function.

ALL STAKEHOLDERS

- Engage in a new debate about how compliance with Sections 302 and 404 of SOX is or should be evolving to meet shareholder and market understandings and expectations.

Stakeholder Consultation for This Paper

In the development of this paper, The IIA sought to obtain a broad range of diverse perspectives across the internal audit profession. In Q3 and Q4 of 2025, The IIA convened a SOX Working Group, consisting of experienced audit professionals and subject matter experts. Over the course of several months, the group met four times to debate and reflect upon the issues organizations face in complying with SOX, as well as the relationship between internal auditing and SOX.

In addition to the SOX Working Group, The IIA held a six-week stakeholder consultation in October and November 2025 wherein all interested parties were invited to submit their views, ideas, and suggestions for this paper.[18] All feedback was carefully considered and discussed, leading to a final version of this paper which was presented to the SOX Working Group in January 2026 for additional review, critique, and comment.

Subsequently, a final version of this paper was presented to The IIA's North American Board for discussion, critique, and approval on January 28, 2026, and to The IIA's Global Board of Directors on February 9, 2026.

The IIA wishes, in particular, to acknowledge the important contributions of the following individuals as part of the SOX Working Group:

- **Elizabeth Sullivan, CIA, CCSA, CRMA**
  2025–26 Chair of the North American Board of Directors, The Institute of Internal Auditors
  Vice President, Chief Risk and Audit Officer, Washington Metropolitan Area Transit Authority

- **Jose Esposito, CIA, CRMA, CRISC, AML/CA**
  Chief Corporate Audit Officer, Credicorp Ltd.

- **Prashant Karanam**
  Global Internal Controls Leader in the Consulting Practice - Risk Management, the EY global organization

- **Ric Kimball, CIA, CRMA**
  Partner and Service Network Leader, Internal Audit and Controls, KPMG

- **Emiliano Ramos Colmenar, CPA-ROAC, CESGA**
  Chief Audit Executive, Telefónica Tech

[18] For a list of the suggested guided questions for consultation participants, see the Appendix.

- **Okorie Ramsey, CIA, CPA, CGMA, PMP, NACD.DC**
  Vice President of Sarbanes-Oxley, Kaiser Permanente

- **Andrew Struthers-Kennedy, CISA, CRMA**
  Managing Director, Protiviti

These individuals added significant value, offering candid and constructive insights based on their combined decades of experience. The IIA would also like to acknowledge Stacey Schabel, CIA, CPA – Senior Vice Chair of The IIA's Global Board of Directors – for contributing her expertise and insights in the development of this document.

It is important to note that participation in the SOX Working Group should not necessarily be construed as a specific endorsement of the paper nor any of its recommendations by these profession leaders nor the organizations for whom they work. Rather, it is meant to show the diversity of subject matter experts who informed The IIA's deliberations and final recommendations. The views and recommendations in this paper should be viewed as solely those of The Institute of Internal Auditors.

APPENDIX

Model Legislative Language

As set forth in Recommendation #1 of this paper, The IIA submits the following proposed legislative definitions of "internal audit" and "internal audit function" for consideration:

(1) **INTERNAL AUDIT**.— The planning and performing of services which provide risk-based objective assurance, independent from management, over internal controls, information, processes, and systems within an organization, the reporting thereon, and, when provided with such services, related advisory and/or consulting services such as risk mitigation, strategic advice, insight, and foresight, and activities to evaluate and improve the effectiveness of an organization's governance, risk management, and control and compliance processes.

(2) **INTERNAL AUDIT FUNCTION**.— The term "internal audit function" means a professional individual or group within a covered entity who, in conformity with globally accepted internal auditing standards, is responsible for providing: the board of directors, an audit committee, if applicable; and management with: objective assurance over the covered entity's internal controls; consulting services; and strategic advice on risk mitigation. For the purposes of this Act, an internal audit function shall be—

(A) Independent from management, reporting to the entity's board of directors, a committee, or another body to which the board of directors has delegated certain functions;

(B) Led by a qualified professional responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services;

(i) The leader of the internal audit function, and relevant staff, shall hold:

(I) appropriate professional certifications or other credentials, such as the Certified Internal Auditor credential.

(ii) No provision in this Act shall exclude the option of a partially or fully outsourced internal audit function, provided the entity fulfilling the internal audit function does not provide external audit services to the same covered entity.

(C) Required to establish a written internal audit charter agreed upon by both the board of directors and the qualified professional leading the internal audit function.

(D) Subject to:

(i) an external quality assessment performed at least once every five years by a qualified, independent assessor or assessment team; or,

(ii) an external quality assessment met through a self-assessment with independent evaluation.

The Roles and Responsibilities of the Governing Body, Senior Management, and the Internal Audit Function

GOVERNING BODY

- Holds responsibility for the overall strategic direction and success of the organization (e.g., board of directors, board of trustees, city council, etc.)
- Maintains accountability for management activities, including compliance with legal, regulatory, and ethical expectations
- Establishes and oversees an independent, objective, properly resourced, and competent internal audit function
- Approves the internal audit charter, which defines the function's authority, role, and responsibilities

SENIOR MANAGEMENT

- Leads and directs the execution of organizational objectives set forth by the governing body
- Establishes and maintains appropriate structures and processes for the management of operations and risk (e.g., CEO, CFO, CTO, senior management team, etc.)

INTERNAL AUDIT

- Maintains direct accountability to the governing body (or its audit committee) and independence from management
- Provides independent and objective assurance over internal controls and strategic advice to promote the improvement and achievement of organizational objectives
- Led by the chief audit executive or an internal auditor with a similar title/role

Key: Accountability, reporting | Delegation, direction, resources, oversight | Alignment, communication, coordination, collaboration


Internal Audit Functions:
Low Cost,
Positive Impact
The Cost of Effective Internal Audit
Many assume internal audit is expensive, but it costs less than 1% of a company's revenue – a small investment for significant risk protection. Internal auditors save time and reduce burdens by proactively identifying risks and ensuring effective controls, enabling governing bodies to focus on strategic goals and shareholder value.
At less than 1% of revenue, internal audit isn't just cost-effective – it's a competitive advantage.
Benchmark data from
158 publicly traded companies
with internal audit functions (in-house or outsourced) shows that
91% spend less than 0.8% of revenue.
With emerging technologies like
AI and data analytics,
internal audit budgets will become even more efficient, shifting focus to specialized skill sets rather than outdated processes.
Internal audit teams range in size from
micro (1-3 auditors) to very large (50+).
Why Internal Audit Matters
Independent & Objective
Reports directly to the audit committee, providing an unbiased view of risks beyond financial reporting, including cybersecurity, fraud, supply chain, and data privacy.
Investor & Public Confidence
Strengthens oversight of operational, compliance, and reporting controls, reinforcing trust among investors, regulators, and stakeholders.
Risk-Based & Cost-Effective
Focuses on critical risks, preventing costly surprises and optimizing resource allocation.
Beyond Compliance: A Strategic Asset for Leadership
Empowers the Audit Committee
Delivers timely insights and risk assessments, enhancing strategic oversight.
Optimizes Budgeting & Risk Management
Aligns audit resources with organizational priorities, ensuring cost-effective risk mitigation without a one-size-fits-all approach.
Encourages Cross-Functional Collaboration
Works with management and key departments to prioritize risks and leverage emerging technologies for more efficient audits.

Recommended Questions From The IIA's Stakeholder Consultation

The following recommended questions guided The IIA's six-week stakeholder consultation process in the Fall of 2025:

1) Internal audit is instrumental in providing organizations with the objective assurance needed to comply with Sections 302 and 404 of SOX. Given this important responsibility, should internal audit's role be mentioned in the law?
2) The cost of complying with SOX is of particular interest to Congress. With this context in mind, does internal audit have the potential to reduce compliance costs? If so, can you provide examples or evidence from your experience?
3) Are there specific provisions of SOX that impede the work of internal auditors? If so, please list each section and describe how the law negatively impacts the profession. Do you have any recommendations on how the language can be improved?
4) Are there any sections of SOX you have found that either directly or indirectly conflict with The IIA's International Professional Practices Framework®? If so, please identify the section, describe the conflict, and suggest how alignment could be improved.
5) Beyond the passage of SOX into law, are there issues or concerns related to the Public Company Accounting Oversight Board, its regulations, operations, or guidance which directly impact the internal audit profession and/or its ability to support compliance with SOX?
6) What other policy opportunities exist – beyond those already mentioned – to promote the role of internal audit in SOX?
7) Do you have any other thoughts concerning the intersection between SOX and internal audit?
8) While SOX is a U.S.-based law, it has had a global influence. At the same time, other countries have sought their own policy solutions to regulate external financial audits and protect investors. What insights from other countries' approaches could improve SOX and external audits and their relation to internal auditing?

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 260,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit theiia.org.

Disclaimer

Copyright

2026

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101