KPMG

The Future of SOX
A point of view for 2030 and beyond

How AI is reshaping SOX, ICFR, and Internal Audit for the next era of assurance

How may artificial intelligence (AI), especially generative AI and agentic technologies, reshape Sarbanes-Oxley (SOX) compliance and internal control over financial reporting (ICFR) by 2030 and beyond?

This article explores how these technologies could transform the design, execution, monitoring, and assurance of internal controls, helping SOX leaders, finance executives, risk and compliance professionals, and audit committees prepare for the next wave of change.

Contents

Introduction: SOX at an inflection point

For more than two decades, SOX compliance has been a cornerstone of confidence in US capital markets. But the model that defined SOX for most of its history—periodic assessments, manual evidence collection, sample-based testing, and heavy reliance on human intervention—is reaching its limit.

A faster, more digital, AI-enabled business environment is forcing a fundamental reset.

SOX is no longer evolving at the margins. It is shifting from a periodic compliance exercise to a continuous, automated, and increasingly predictive capability embedded within the business itself. That shift is driven by three converging forces:

01 The digitization of core finance processes

02 Pressure to improve efficiency and insight

03 The rapid advancement of artificial intelligence—especially generative AI and agentic technologies.

2025 SOX Survey excerpts

- The cost of maintaining SOX controls rose 45 percent between our 2023 and 2025 surveys.
- Average testing hours per control increased from 12 hours in fiscal year (FY) 2022 to 16 hours in FY 2024, with transactional and information technology general controls requiring the most time to test.
- Only 28 percent of companies polled used outsourced providers for SOX testing, but …
- 58 percent indicated that outsourced providers accounted for more than 20 percent of their SOX program budget, indicating continued support for cosourcing.
- 52 percent of Internal Audit departments dedicated more than 40 percent of their total Internal Audit hours to SOX compliance in FY 2024, indicating that for most organizations SOX was a significant part of their overall Internal Audit workload.

Source: The 2025 SOX Survey, KPMG LLP

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

The implications extend far beyond efficiency. One expectation of AI is the possibility of decreasing the cost of overall compliance, which has been steadily rising over the past few years, according to a recent KPMG survey (see insert, *2025 SOX Survey excerpts*).

In the years ahead, leading organizations will distinguish themselves not by reducing control counts, but by building control environments that are more automated, more risk-responsive, and more resilient. In practice, this means relying more heavily on automation and testing approaches that are clearly tied to risk assessment, rather than equating optimization with simplification alone.

This will require a new model for ICFR programs—one grounded in stronger AI governance, control monitoring embedded within the business (i.e., first line of defense), scalable testing, and a workforce fluent in both audit judgment and technology.

This white paper outlines the five points of view that KPMG believes will define the future of SOX, explores how the ICFR function must evolve in response, and offers a practical call to action for organizations that intend to lead this transformation rather than react to it:

- **The governance of AI** 1
- **Embedded and autonomous controls** 2
- **Scalable AI-enabled testing** 3
- **AI as a guide through transformation** 4
- **Evolving role of the ICFR function** 5

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Point of view 1

The governance of AI

A new SOX frontier: auditing AI itself

A significant development that is already facing auditors, in addition to AI as a tool for auditors, is AI as the subject of the audit. As organizations embed AI models, generative AI copilots, and autonomous agents into financial workflows, a critical new mandate will emerge—providing meaningful assurance over the AI systems themselves.

Today, most ICFR programs assess controls over financial data, business processes, and the systems that support them. Tomorrow, those programs will need to extend their perimeter to include the AI systems that increasingly generate, transform, and validate that data. The integrity of financial reporting will depend, in part, on the integrity of the models that underlie it.

> The industry has largely avoided AI-related material weaknesses to date—not because the risks aren't real, but because organizations with strong AI governance capabilities within their ICFR functions have been able to stay ahead of them. That may not last.
>
> — Charles King, AI Technology Leader, Internal Audit & Controls, KPMG LLP

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

The first AI-related material weaknesses

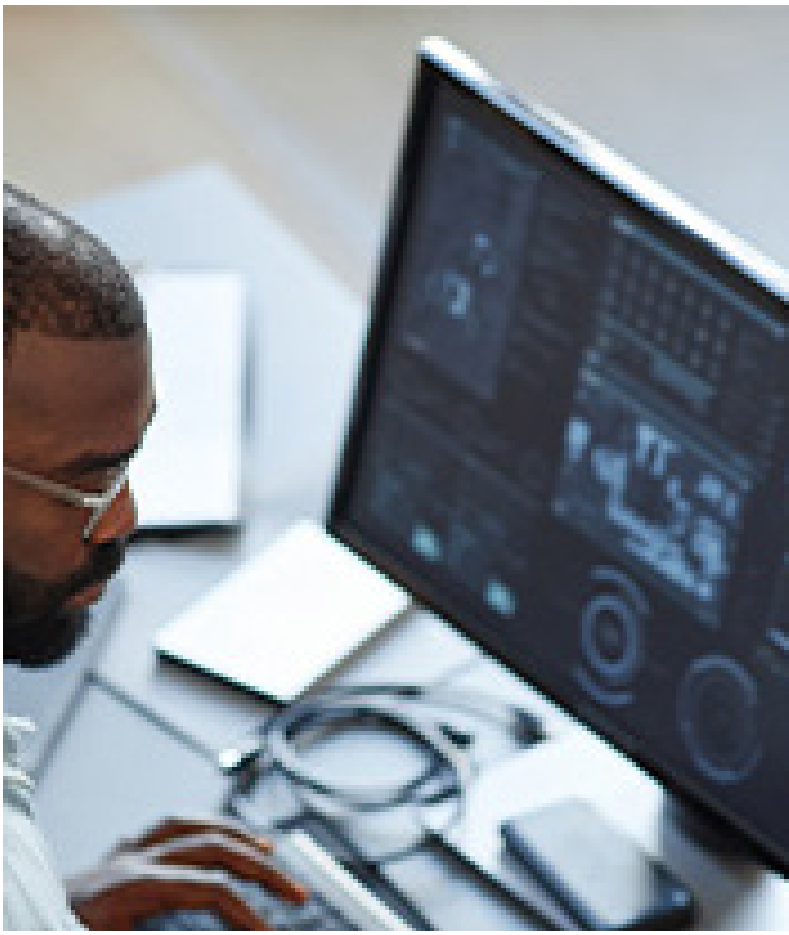
The industry has largely avoided AI-related material weaknesses to date—not because the risks aren't real, but because organizations with strong AI governance capabilities within their ICFR functions have been able to stay ahead of them. This may be a factor of timing. Because the AI models are still new, the SOX programs haven't fully started relying on those controls and are still testing "around" the AI, relying on manual and other automated controls that still get us there. Likely during this next year, it will start to be unavoidable to work AI considerations into the control environment, which may open those processes up to material weaknesses (MWs). We expect to see the first wave of MWs appear in 2027.

Consider one illustrative scenario: An error occurs within an AI system that influences a delegation-of-authority workflow, resulting in approvals that fall outside established policy thresholds. In a poorly governed environment, such an event, if occurring repeatedly, could compromise the integrity of expenses authorized by the company, potentially triggering a reportable control deficiency. These are not hypothetical concerns; they are predictable failure modes in systems that have not been adequately controlled.

Leveraging established frameworks

Addressing AI governance within SOX requires organizations to ground their efforts in established and emerging frameworks. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) publication on generative AI,[1] which extends the 2013 *Internal Control – Integrated Framework* into the realm of generative AI, provides a critical reference point. By aligning AI governance practices with COSO-recognized principles across the five components of internal control—control environment, risk assessment, control activities, information and communication, and monitoring activities—organizations can build an AI oversight structure that is both rigorous and auditable.

KPMG believes the organizations that will lead on AI governance are those that resist the temptation to treat it as a separate workstream and instead integrate it seamlessly into their existing ICFR infrastructure.



[1] Scott Emett, et al., "Achieving Effective Internal Control Over Generative AI," Committee of Sponsoring Organizations of the Treadway Commission, 2026.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Point of view 2

Embedded and autonomous controls

The rise of "self-healing" controls

For decades, internal control design has relied on a combination of preventive controls—configurations, system rules, and approval workflows—and detective controls—reconciliations, exception reports, and management reviews—to protect financial integrity. The balance between these two approaches has always tilted toward the detective side, because building truly effective preventive controls requires deep system integration and ongoing maintenance.

AI changes that calculus. The next generation of controls will be preventive, embedded, and—increasingly—self-healing. Rather than waiting for a control to alert users that a server does not have the correct configuration, tomorrow's control environments will be configured to identify, flag, and in some cases automatically correct this anomalous condition in real time before it can introduce the possibility of errors in financial reporting.

These self-healing controls are not passive configurations. They are dynamic learning systems that monitor process behavior against established baselines, adapt to evolving risk patterns, and escalate exceptions to human reviewers only when intervention is genuinely required.

Reduced reliance on manual intervention

The practical consequence of this shift will be a significant reduction in the reliance on manual and detective controls. This is not merely an efficiency gain—though the efficiency gains will be substantial. It represents a fundamental improvement in the reliability of the control environment. Human error, which remains one of the most persistent drivers of control deficiencies, is significantly reduced when critical checkpoints are embedded in automated workflows rather than dependent on individual execution.

For ICFR functions, this means that the nature of control testing will change as well. Testing an embedded, automated control requires a different methodology than testing a manual review: It demands an understanding of system configuration, data logic, and the conditions under which automation may fail or be bypassed. The auditor of the future must be as comfortable in a system configuration log as in a transaction ledger.

> The next generation of controls will be preventive, embedded, and—increasingly—self-healing. Rather than waiting for a reconciling item to surface in a monthly close, tomorrow's control environments will be configured to identify, flag, and in some cases automatically correct anomalous conditions in real time before they can affect the accuracy of financial reporting.

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Point of view 3

Scalable, AI-enabled testing

From sampling to full population testing

Traditional SOX testing has long been constrained by sampling. Because modern enterprises process such large volumes of transactions, human auditors have only been able to review a small portion of the total population. As a result, audit conclusions have always included an inherent limitation: The sample tested showed no evidence of control failure, but not every transaction was examined.

AI and other technologies can facilitate exactly that. Where appropriate, digitally enabled testing will allow both management and external auditors to examine 100 percent of transactions within scope—not on an annual basis, but continuously. External auditors and practitioners are already doing this with certain types of transactions. However, we expect that a more broad-based shift from periodic, sample-based testing to ongoing full-population assurance will represent one of the most significant advances in audit methodology since the advent of computerized accounting systems.

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Continuous, real-time assurance

Full population testing is not an end in itself—it is the enabler of something even more valuable: continuous, real-time assurance over the control environment. Rather than issuing a point-in-time opinion on whether controls were effective for the prior fiscal year, the ICFR function of the future will provide a living, dynamic view of control health across the enterprise.

This capability also clarifies an important distinction in the three lines of defense model–particularly when the Internal Audit department plays a large role in the SOX program. The first line—business process owners and managers who operate controls daily—will increasingly leverage continuous monitoring tools to track control effectiveness in real time as part of their operational responsibilities. The third line—internal audit—will focus on testing and validating what the first line is doing: independently assessing the reliability of those monitoring processes, rather than reperforming the operational work.

Maintaining clarity around this boundary is critical. The value of Internal Audit depends on its independence, and that independence is best preserved when the first line owns operational monitoring and the third line owns the testing of monitoring itself. Nevertheless, we believe that SOX programs should be focused on providing meaningful input and guidance to the first line of defense. Independence should not become the sole basis for internal auditors to limit themselves to purely reporting control effectiveness or ineffectiveness.

Automating evidence collection

Continuous automated testing cannot be achieved without continuous evidence collection. Manual provided by client (PBC) processes—the time-consuming back-and-forth of requesting, compiling, and submitting control support—are fundamentally incompatible with the speed and scale that AI-enabled testing demands.

Organizations best positioned to realize the benefits of AI-enabled assurance have already moved to automated evidence collection. They embed control evidence in process workflows, store it directly in enterprise systems, or maintain it in standardized repositories that automated tools can access and analyze without manual intervention. Investing in this infrastructure is not just a near-term efficiency gain; it is a foundational step toward unlocking the full value of AI-driven assurance. In fact, for some teams, focusing on automated evidence collection may even represent a more immediate opportunity for return on investment than automated testing.

Rather than issuing a point-in-time opinion on whether controls were effective for the prior fiscal year, the ICFR function of the future will provide a living, dynamic view of control health across the enterprise.

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Point of view 4

AI as a guide through transformation

Synthetic data as a risk intelligence tool

Among the most innovative applications of AI in the ICFR context is the use of synthetic data—artificially generated datasets that mirror the statistical properties of real transaction populations—to anticipate where control gaps and risks may emerge before live data is ever involved.

This capability is particularly powerful in the context of system implementations and merger and acquisition transactions, two scenarios that have historically been among the highest-risk environments for financial reporting integrity. When an organization is migrating to a new enterprise resource planning platform or integrating an acquired company's systems and processes, the window between go-live and the establishment of a stable, well-tested control environment represents significant exposure.

Synthetic data testing allows organizations to pressure-test that window in advance. By introducing synthetic transaction populations into a new system—say, an acquired company's data flowing through a new ERP environment—organizations can observe how controls respond, identify unexpected failure modes, and remediate gaps before real financial data is at stake. This transforms risk assessment from a reactive exercise into a proactive one.

Using AI, synthetic data can closely replicate the types of data that are actually generated, giving organizations a better chance of identifying anomalies and process glitches.

AI agents to pressure-test new environments

Related to the use of synthetic data is the concept of deploying AI agents specifically to stress-test control environments. These agents can be configured to simulate the behavior of users, transactions, and system events across a range of scenarios—including edge cases and adversarial conditions that human testers might not anticipate.

In the context of a system implementation, such agents can effectively recreate the roles and interaction patterns expected in the live environment, revealing how access controls, approval workflows, and automated rules perform under conditions of scale and variability. In the context of an acquisition, AI agents can model the integration of the acquired entity's risk profile into the acquirer's control framework, surfacing potential conflicts or gaps well before the integration is complete.

This is not merely a testing technique—it is a new form of risk intelligence, one that turns the power of AI against the risks that AI itself introduces.

> Synthetic data testing allows organizations to pressure-test that window in advance. By introducing synthetic transaction populations into a new system.
>
> — Charles King, AI Technology Leader, Internal Audit & Controls, KPMG LLP

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Point of view 5

The evolving role of the ICFR function

Beyond external auditor reliance

For many years, one of the primary value propositions of a robust internal controls program has been its potential to support external auditor reliance—the idea that a well-functioning ICFR function reduces the extent of independent testing that external auditors must perform, resulting in audit efficiency and cost savings. This dynamic is likely to shift meaningfully in the coming years.

As external audit firms deploy their own AI solutions to perform control testing at scale, the marginal value of relying on management's testing may diminish—at least in lower-risk areas. When an external auditor can test 100 percent of a transaction population using automated tools, the incremental assurance value of management's 25-item sample test is limited.

However, the inverse is also possible. If an organization's internal AI-enabled testing capabilities are sufficiently sophisticated—providing a demonstrably higher level of assurance than the auditor's own tools—the external auditor may place greater reliance on management's work, not less. The future of audit reliance may come down to a question of technological capability: a race to develop AI-powered testing tools that meet the evidentiary bar required for financial statement purposes. Regardless of the extent of reliance, management will be well advised to use their digital capabilities to identify and resolve potential issues before they are detected by external auditors.

This uncertainty argues strongly for organizations to invest in their ICFR technology capabilities now, positioning themselves as leaders in the eventual equilibrium rather than fast followers.

As external audit firms deploy their own AI solutions to perform control testing at scale, the marginal value of relying on management's testing may diminish — at least in lower-risk areas.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

From auditor to strategic advisor

The professional identity of the SOX professionals is also undergoing a transformation. The traditional model—CPAs with deep accounting knowledge who are trained to follow audit methodology and assess control design and effectiveness according to established standards—remains foundational, but it is no longer sufficient on its own.

The ICFR function of the future will require professionals who are simultaneously fluent in accounting standards and AI systems, risk frameworks and data science, traditional audit methodology, and emerging technology risk. The function's value will increasingly lie in its ability to synthesize these domains—providing strategic advisory services on control design, AI governance, and risk management that go far beyond traditional audit findings and recommendations.

This is a shift from assurance to insight. The SOX practitioner of 2030 will not simply tell management whether a control worked; they will advise on how the control should be redesigned to work better in an AI-enabled environment, and they will bring the technical depth to make that advice credible.

A new skillset for a new era

This transformation has material implications for talent strategy. Today's model—recruit accounting graduates, train them in audit methodology, and develop them through years of client service—will not produce the professionals the function needs at scale. The skills required to audit an AI system, assess a language model's reliability, or evaluate the adequacy of a synthetic data testing program are not currently core to the CPA curriculum.

Forward-looking organizations are already experimenting with alternative talent models: data scientists who specialize in audit, AI engineers who develop domain expertise in financial reporting risk, and professionals with dual credentials in technology and accounting.

The growing consensus in the profession is that the future of the ICFR function will require individuals who deeply understand both the business process and the technology that underlies it—and that achieving this at scale will require a fundamentally different approach to hiring, development, and professional credentialing.

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Challenges on the horizon

The opportunities presented by AI in the SOX and ICFR context are real and significant. But they arrive alongside a set of challenges that are equally real and should not be minimized. These include:

Auditing the "Black Box." Many AI models—particularly large language models and deep learning systems—do not produce outputs that are easily explained or audited using traditional methods. The question of how to assess the reliability of a control that operates through a complex model is one that many organizations have not yet fully resolved. The lack of widely accepted methodologies for auditing black-box systems remains an open challenge in this space. KPMG has separately published useful guidance on controls and governance in AI systems.

The human-in-the-loop imperative. As controls become more automated, the question of what constitutes meaningful human oversight becomes both more important and more difficult to answer. A human approval step that rubber-stamps every AI recommendation provides no real control value. Defining the conditions under which human judgment adds genuine risk-reduction benefit—and designing oversight mechanisms that reliably capture that benefit—requires careful thought and ongoing experimentation.

New and amplified risks. AI introduces a new landscape of risks that traditional ICFR frameworks were not designed to address. Model drift, the gradual degradation of a model's performance as the data environment evolves, can cause a control that was effective at implementation to become ineffective over time, without any visible change in the system. AI bias can systematically distort outputs in ways that affect the fairness and accuracy of financial reporting. Prompt-injection attacks, in which malicious inputs are used to manipulate AI model outputs, represent a novel cybersecurity risk with direct financial reporting implications. This is not purely an external risk. Unscrupulous control owners who are aware that auditors are using AI to test controls may be tempted to hide language in control evidence that directs the testing agents to overlook evidence that may indicate an ineffective control.

Regulatory disclosure requirements. Both the Public Company Accounting Oversight Board and the Securities and Exchange Commission are actively developing their thinking on disclosure requirements related to AI in financial systems and controls. Organizations should expect greater scrutiny over how AI is being used in financial reporting processes, the risks those uses introduce, and the controls established to govern them. Internal audit and ICFR functions may have an increasingly significant role to play in supporting the integrity, completeness, and defensibility of those disclosures.

Third-party and vendor risk. Many organizations rely on third-party vendors for core financial technology, and those vendors are increasingly integrating AI into their own systems and processes. The traditional SOC report review framework was not designed to assess AI-specific risks, and organizations will need to develop more sophisticated approaches to evaluating the adequacy of vendor AI governance—moving away from checkbox compliance toward substantive risk assessment.

> "As controls become more automated, the question of what constitutes meaningful human oversight becomes both more important and more difficult to answer."
> — Sue King, Former US SOX Solutions Leader, KPMG LLP (retired)

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Seizing the opportunity

The challenges outlined above are genuine, but they should not obscure the substantial opportunity that AI presents for the ICFR function. Organizations that approach this moment strategically—investing in technology, talent, and governance infrastructure now—stand to reap significant benefits.

These benefits include, but are not limited to:

Enhanced assurance

Full population testing and continuous monitoring will fundamentally raise the level of assurance available over the control environment. Organizations will be able to demonstrate—not merely assert—that controls are operating effectively, and do so on a continuous basis rather than at a point in time. This is a qualitatively different kind of assurance: more reliable, more defensible, and more valuable to the board, management, and external auditors who depend on it.

Strategic value add

As AI assumes a greater share of transactional audit work—data collection, testing, exception identification—the professionals who make up the ICFR function will be freed to focus on higher-value activities: control design advisory, risk management strategy, governance oversight, and the kind of qualitative judgment that no AI system can replicate. This is not a threat to the profession—it's an upgrade to it.

Proactive risk management

Most significantly, AI-enabled continuous monitoring transforms the ICFR function from a reactive to a proactive posture. Rather than discovering control failures after the close, organizations could identify and address emerging risks in real time—before they can compound into material issues. The shift from a once-a-year control assessment to a continuous risk intelligence capability represents a fundamental improvement in organizational resilience.

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Call to action

Preparing for the future

The transformation described in this white paper is not a distant prospect. It is already underway, and the organizations that begin building their capabilities today will have a decisive advantage over those that wait. We recommend the following three-phase approach structured around three horizons of action.

Phase 1: Foundational steps

Craft a bold AI strategy. Develop a clear and ambitious roadmap for how your organization will adopt, scale, and govern AI within your ICFR programs. This strategy should be grounded in business risk priorities, aligned with enterprise AI governance initiatives, and informed by the emerging regulatory landscape. Ambiguity about AI strategy is itself a risk; clarity is a control.

Invest in talent. Begin cultivating and recruiting AI-literate talent within your audit, compliance, and risk functions now. This does not mean replacing experienced auditors with data scientists overnight—it means building bridges between these disciplines, creating development pathways for current staff, and opening hiring channels to professionals with nontraditional backgrounds.

Conduct a controls clean-up. Before layering AI onto an existing control environment, invest the time and effort required to ensure that environment is sound. This means:

- Ensuring management owns and can clearly articulate each control and its relationship to the broader risk landscape
- Treating controls integration as an ongoing process, not a one-time event
- Reviewing controls to ensure they are well-defined, explicitly linked to the risks they are designed to mitigate, and categorized appropriately
- Verifying that control testing procedures are properly aligned with control objectives and supported by strong documentation.

AI amplifies what it finds: A poorly designed control environment will not be improved by automation—it will be magnified.

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Phase 2: Building momentum

Focus on measurable outcomes. Deploy AI solutions that are linked to your enterprise's strategic priorities and can demonstrate measurable results—reduction in testing cycle time, increase in population coverage, and improvement in exception identification rates. Resist the temptation to pursue AI for its own sake; pursue it in service of specific, defined objectives.

Establish robust governance. Build the governance infrastructure—policies, standards, oversight mechanisms, and change management processes—that will allow your AI initiatives to scale responsibly. Wherever possible, default to general enterprise AI governance policies and processes. This scaffolding is not glamorous, but it is the difference between an AI initiative that delivers sustained value and one that creates the very risks it was meant to reduce.

Phase 3: Achieving transformation

Redesign for AI-enabled capacity. Fundamentally rewire your ICFR strategy and operating model to incorporate AI agents as core contributors alongside human professionals. This means rethinking workflows, redefining roles, and creating new accountability structures that are fit for an AI-enabled environment rather than adapted from a human-only one.

Foster organizational agility. The organizations that will thrive in the AI era are those that can move quickly, learn continuously, and adapt at pace with an evolving technology landscape. This requires flatter organizational structures, empowered multiskilled teams, and a culture that treats experimentation as a core competency rather than a risk to be managed. The ICFR function of the future will not be built through top-down mandates; it will be built through the cumulative innovations of teams that have the skills, the tools, and the freedom to lead.

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

Conclusion

SOX was born from a crisis of confidence in financial reporting. Its purpose was clear: restore trust through disciplined controls, accountability, and independent assurance. That mandate has not changed. What has changed is the environment in which those controls now operate.

AI does not reduce the need for SOX—it raises the stakes. As financial processes become more digital, more automated, and more dependent on intelligent systems, organizations will need controls that are stronger, faster, and more adaptive than the ones that carried them through the last two decades. The future of SOX will belong to organizations that can pair innovation with governance, automation with assurance, and technological speed with sound judgment.

This is the next inflection point for ICFR programs. The shift is already underway, and the cost of waiting will only increase. The question is no longer whether AI will reshape the control environment. It is whether your organization will move early enough to shape that future with intent—or be forced to catch up to it later.

> AI does not reduce the need for SOX—it raises the stakes.
> — Charles King, AI Technology Leader, Internal Audit & Controls, KPMG LLP

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A

How KPMG can Help

KPMG offers a range of capabilities to help organizations modernize their SOX programs and prepare for an AI-enabled future, including:

01

AI readiness and technology strategy

Our SOX and technology professionals work with organizations to identify where AI, agents, and enabling technologies can create meaningful value. We help define practical roadmaps, prioritize use cases, and align investment decisions to business objectives, risk appetite, budget, and technology maturity.

02

AI implementation and enablement

KPMG brings deep experience implementing AI and agentic technologies across enterprise environments. With alliances across major cloud providers and software vendors, we help organizations move with speed, strengthen governance, and improve the effectiveness of their SOX programs.

03

SOX program health check

We assess program design, operating effectiveness, cost, and collaboration models against peer practices and objective benchmarks to identify targeted opportunities for improvement.

04

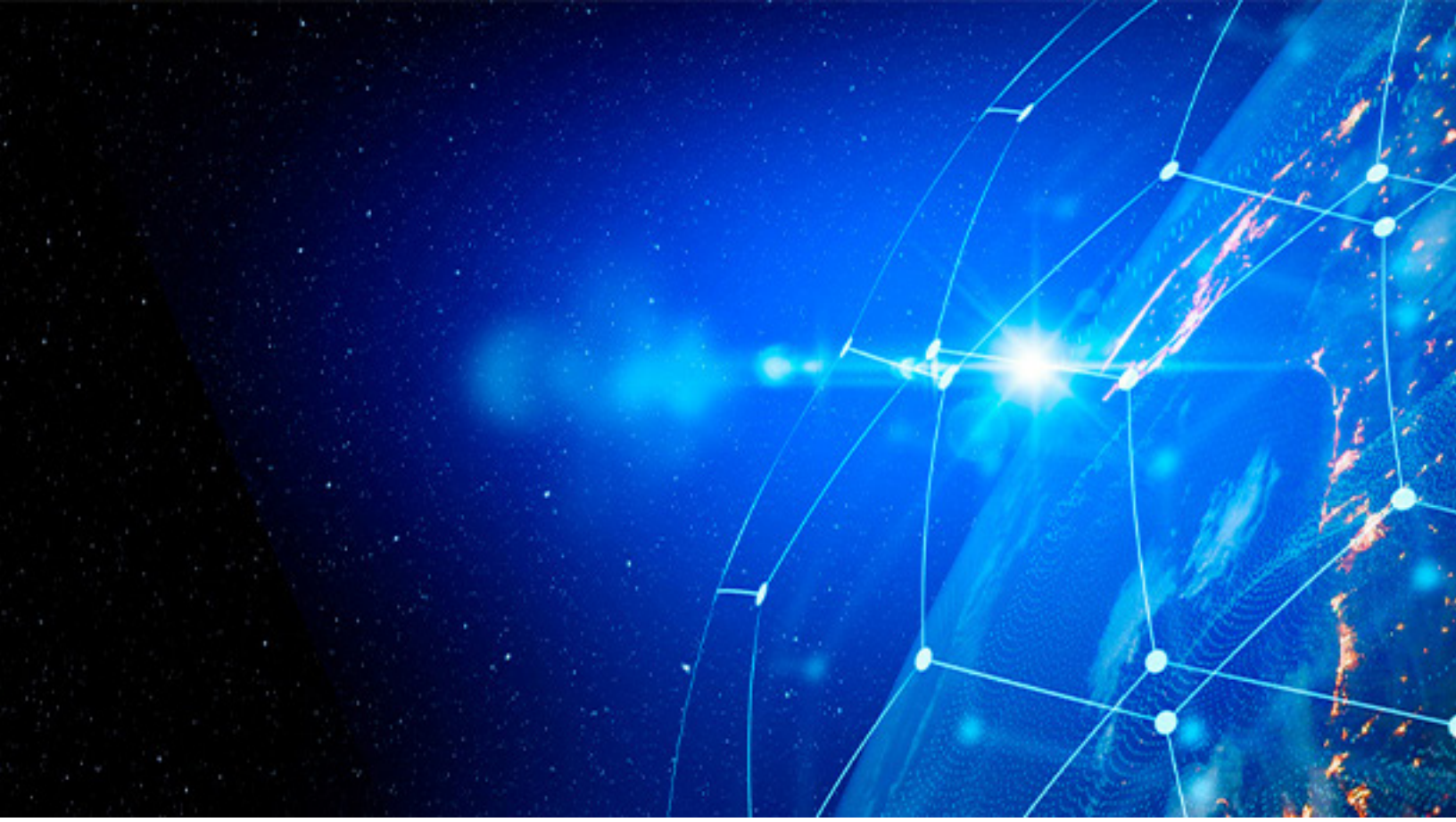
SOX cosourcing

Our experienced professionals help organizations scale delivery, strengthen execution, and maintain focus on the business while enhancing trust, quality, and cost discipline across the SOX program.

At KPMG, we believe AI will play a defining role in the future of SOX compliance—making programs more efficient, more adaptive, and more insightful. We also recognize that the path forward is complex and requires clear governance, practical execution, and sustained investment.

Whether your organization is exploring the first practical uses of AI or pursuing broader transformation, KPMG can help you move with greater clarity, confidence, and control.

KPMG © 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043535-1A



Contact us

Ric Kimball
Internal Audit & Controls Service Line Leader
KPMG LLP
ekimball@kpmg.com

Charles King
AI Technology Leader, Internal Audit & Controls
KPMG LLP
crking@kpmg.com

Michael Smith
Internal Audit & Controls Growth Leader
KPMG LLP
michaelasmith@kpmg.com

Subash Samuels
Principal, Internal Audit and Controls Services
KPMG LLP
ssamuels@kpmg.com

Discover more at visit.kpmg.us/FutureOfInternalAudit

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS043535-1A