KPMG

Beyond the Checkbox:
How Confident Are You in Your SOC 2 Reports?

kpmg.com/us

Introduction

As businesses increasingly rely on third-party vendors, a System and Organization Controls (SOC) 2 report is an indispensable asset for building and maintaining customer trust. The pressure to obtain a SOC 2 report has led to the rapid adoption of SOC 2 Tool Providers[1] and the emergence of new entrants in the SOC 2 audit space. While these trends have made SOC 2 reports more accessible, they compel Chief Information Security Officers (CISOs) and others charged with cybersecurity governance to look beyond the compliance certificate and ask a more critical question:

> **"How confident are you in the quality and accuracy of your SOC 2 reports?"**

This white paper explores the evolving SOC 2 landscape and provides a guide for leaders to navigate it effectively. Key topics covered include:

SOC 2 Tool Providers

Automated compliance platforms may offer efficiency but introduce risk when relied upon without sufficient validation, as they may confirm control existence without addressing effectiveness within the organization's specific risk environment.

The Irreplaceable Role of the Auditor

Experienced auditor judgment remains essential to deliver meaningful, context-driven evaluations, addressing gaps that automation alone cannot cover.

A Guide for Critical Evaluation

Effective use of SOC 2 reports requires disciplined evaluation of scope, testing rigor, and findings to assess the reliability of conclusions and their relevance to organizational risk.

[1] A "SOC 2 tool provider" is a vendor that supplies software or services that service organizations use to help design, operate, and monitor the effectiveness of controls and to support reporting, in conjunction with SOC 2 readiness and ongoing compliance activities. Source: SOC engagements: Ethics risks with tool providers

© 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. USCS042683-1A

The Rise of SOC 2 Tools

A Partnership of Automation and Expertise

The emergence of automated compliance platforms has brought significant efficiency and accessibility to the SOC 2 process, and they are assets for organizations preparing for an audit. Typically, these SOC 2 tools integrate directly with a company's cloud services and SaaS applications to automatically collect evidence, continuously monitor hundreds of technical controls, and manage policy documentation. Like any tool, however, their value is maximized when their capabilities and boundaries are fully understood. Whether you are selecting an auditor for your own organization or evaluating a SOC 2 report from a critical vendor, this means recognizing where these SOC 2 tools excel and where the nuanced judgment of an experienced auditor remains irreplaceable.

This section explores the benefits and areas of consideration to help leaders build a comprehensive compliance strategy that leverages the best of both automation and human expertise.

Benefits of Automated Audits

Speed and Efficiency:
Automation can accelerate the evidence-gathering process, reducing the time and internal resources required for an audit.

Cost-effectiveness:
By streamlining many of the manual tasks associated with audits, these platforms may make SOC 2 compliance more affordable, especially for smaller businesses.

Continuous Monitoring:
Many platforms provide ongoing monitoring of controls, enabling companies to maintain a state of continuous compliance.

Areas of Consideration

Focus on Coverage and Configuration:
Automated tools are very effective at validating configuration states for known assets. For example, a tool may confirm encryption is "enabled" for the databases it monitors, but additional governance and validation are needed to determine relevant databases across the environment are monitored and corrective action is taken when exceptions are identified.

Business and Technical Context:
Security is not one-size-fits-all. SOC 2 tools typically use standardized mappings and integrations, which means they may not fully reflect an organization's unique business logic, data flows, and architectural nuances without thoughtful configuration and interpretation. A control that is adequate for one company may be insufficient for another—a distinction that is best addressed through human judgment, interviews and risk-based testing in conjunction with the SOC 2 tool's automated testing.

Keep Strategic Risk Management Front and Center:
Automated dashboards provide visibility into key data points and control signals; however, these metrics may be unreliable without a robust risk assessment. For example, a risk assessment that does not address and respond to risks related to security, configuration and data changes, information integrity, and the reliability of outputs may lead to misleading conclusions, ineffective decision making, and a false sense of control effectiveness.

It is important to remember that these SOC platforms are tools and not substitutes for a comprehensive security program. They can be valuable for organizing evidence and managing controls, but cannot replace the critical thinking and professional judgment of an experienced auditor.

© 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. USCS042683-1A

Selecting the Right Auditor

Translating Data into Assurance

Selecting the right audit partner is crucial for an effective and meaningful SOC 2 engagement. The audit process is an opportunity to identify areas for improvement and strengthen your security posture.

Here is what to look for to distinguish a strategic audit partner from one that applies a more templated approach that may not fully reflect the complexities of the organization:

A Risk-based and Contextual Approach

This begins, with a deep discovery process where the auditor understands your unique business risks, data flows and technology. This allows them to focus on risks and the "why" behind your controls—their purpose and function—not just "what" is in place. This understanding allows tests of controls to be tailored to determine that risks are being addressed appropriately.

From Data to Judgment

An auditor views data from an SOC 2 tool as a starting point, not the final answer. By letting the tool handle data collection, they can focus their time on control execution and management oversight activities, ultimately translating the tool's raw data into a judgment about your actual business risks.

Relevant Industry and Technical Expertise

Verify the firm has experience with companies of your size, industry and complexity. For example, a checklist driven, point in time auditor may simply verify that branch protection rules are enabled in your development repositories. An in-depth technical auditor will understand these protections can be turned on and off; they will investigate whether monitoring controls are in place to validate that these rules have been consistently enforced throughout the audit period.

A Dialogue Driven Approach

A strategic audit partner is willing to engage in thoughtful discussions, provide clarifications and offer constructive feedback that helps you genuinely improve your security posture.

Furthermore, organizations must assess auditor independence when evaluating whether a prospective audit partner remains independent while using a SOC 2 tool provider with which it has a business relationship. As highlighted in a recent ***Journal of Accountancy*** **article ("SOC engagements: Ethics risks with tool providers," April 2026)**[2], there are growing ethical risks when audit firms have complex partnership structures with tool providers. Additionally, this article notes that the most common independence threats for auditors engaged in business arrangements with tool providers are undue influence and self-interest.

While maintaining compliance with AICPA independence standards is the auditor's professional duty, the consequences of a violation – a loss of the report's credibility —fall on the organization being audited. Therefore, always question prospective auditors on how they maintain strict independence and mitigate any potential conflicts of interest when leveraging SOC 2 tool providers with which they have a business relationship.

[2] Source: Journal of Accountancy, "SOC engagements: Ethics risks with tool providers" (April 6, 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. USCS042683-1A

A Guide to Evaluating SOC 2 Report Quality

For vendor risk management functions, receiving a SOC 2 report from a vendor is not the end of due diligence; it's the beginning. The responsibility rests with you, to assess the report's quality and determine if it provides the assurance your organization requires.

Here's what to look for:

Analyze the Auditor's Testing Procedures

Look for a detailed description of the tests performed for each control. The quality and rigor of these procedures are so critical that the AICPA[3] has recently issued guidance for peer reviewers to specifically address risks in how SOC 2 audits are performed, reinforcing the need for your own due diligence. When reviewing, pay close attention to three critical areas:

- **The "How" and the "What":** A quality report will clearly describe *what* was tested, *how* it was tested (e.g. through detailed inspection, observation or re-performance), and what evidence was examined.
- **Over-reliance on Inquiry:** If procedures are heavily limited to "inquiry", challenge how they established the control's effectiveness without observing and/or inspecting evidence.
- **The "Test of One" Fallacy:** Scrutinize reports using a "test of one" approach for testing controls as results may only evaluate the control at a single point in time rather than the operation of the control over a period of time. For example, inspecting a Security Information and Event Management (SIEM) alert proves that a SIEM tool is in use and alerts are generated; however, this procedure does not evaluate if alerts were consistently resolved over the examination period.

Evaluate the Report's Scope and Applicability

Scrutinize the scope of the report to assess whether it covers the specific systems, services and locations that your organization rely on.

Look for Evidence of a Tailored, Risk-based Audit

A quality report will implicitly or explicitly show that the audit was customized to the vendor's specific environment. The system description, the risks identified and the controls tested should tell a cohesive story.

Assess the Clarity and Detail of Findings

Pay attention to any exceptions noted. A quality report will clearly explain the exception, its impact and management's response. A "clean" report does not, by itself, answer every risk question; a thoughtful report with findings can provide stronger insight.

[3] Source: Journal of Accountancy, "AICPA guides peer reviewers to address SOC 2 risks" (May 14, 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. USCS042683-1A

Conclusion

From Compliance to Confidence

Achieving SOC 2 compliance is a significant accomplishment, but not the end goal. The ultimate objective is to build a security program that you, your leadership and end users of the report can be truly confident in. Keep in mind that a thorough validation of a security program requires adequate time. While efficiency is important, very short audit timelines can sometimes limit the depth of discovery and testing needed to fully understand an organization's security posture—especially in complex environments.

By taking a thoughtful approach to the audit process—leveraging automation as a tool, and carefully selecting your audit partner— you can determine whether the SOC 2 reports your organization issues, and the vendors' reports your risk teams rely upon, accurately reflect the security posture of the environment.

Authors

Nina Currigan
SOC Solution Leader
T: 303-382-7808
1225 17th Street, Suite 800
Denver, CO 80202

Nicole Romano
Partner, Audit and Assurance
T: 267-256-1793
1735 Market Street
Philadelphia, PA 19103

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. USCS042683-1A