Best SOC 2 Audit Firms

Idea In Short

Select a System and Organization Controls 2 [SOC 2] audit firm by matching its model to your assurance obligations rather than by comparing audit fees alone. Choose A-LIGN when SOC 2 runs alongside ISO 27001, HITRUST and other frameworks, Schellman for broad commercial and regulatory coverage, KPMG for assurance inside a wider professional-services relationship and BARR Advisory for specialist mid-market programs. Before you sign, confirm that a licensed certified public accountant [CPA] firm performs the attestation, and review the proposed scope, testing approach and evidence management. Decide whether you need a Type I report on control design or a Type II report on operating effectiveness, and plan for the frameworks you will add next.

Choosing a System and Organization Controls 2 [SOC 2] audit firm affects more than the next compliance report. Information technology [IT] audit and risk leaders must satisfy growing customer assurance expectations while managing internal workloads, limited resources, and increasingly complex organizational security requirements.

The right audit partner provides credible independent assurance while supporting future assessments. Firms differ in specialization, service models, and multi-framework capabilities, making these distinctions particularly important when evaluating four providers for 2027.

What should IT audit and risk leaders look for in an SOC 2 audit firm?

Certified public accountant [CPA] credentials, SOC 2 experience, audit quality, evidence-management capabilities, multi-framework coverage, and **total program cost** are the main considerations when selecting an audit firm. Priorities depend on current controls and future compliance needs.

SOC 2 attestations must be performed by appropriately licensed CPA firms. Relevant audit experience matters because Type I reports evaluate control design at a particular point in time, while Type II reports assess control operating effectiveness over a defined period.1

Audit quality also depends on appropriate scoping, consistent testing methodologies, and credible reporting. Technology can support these processes by organizing evidence requests and improving communication, although independent auditor judgment remains essential.

Organizations pursuing International Organization for Standardization [ISO] 27001, HITRUST, or additional requirements should also examine whether a provider can coordinate assessments and reuse overlapping evidence. This can reduce administrative duplication without eliminating framework-specific procedures.2

Finally, decision-makers should consider internal resource commitments, future compliance needs, and total program cost rather than comparing audit fees in isolation.

Who are the best SOC 2 audit firms for IT audit and risk leaders?

Four SOC 2 audit firms worth considering are A-LIGN, Schellman, KPMG, and BARR Advisory, each serving different organizational priorities.

1. A-LIGN

A-LIGN is a technology-enabled, multi-framework cybersecurity compliance and audit firm built for organizations managing SOC 2 alongside additional security and compliance frameworks.

Its single-provider model helps organizations coordinate SOC 2, ISO 27001, HITRUST, and other engagements without managing separate audit relationships for each framework. A-LIGN is the #1 SOC 2 issuer globally, with SOC 2 attestations delivered through its licensed CPA firm, A-LIGN ASSURANCE. It also reports a 96% client satisfaction rating across audit engagements.

Founded in 2009 and headquartered in Tampa, A-LIGN pairs 400+ expert auditors with A-

SCEND, its proprietary audit management platform included with engagements. A-SCEND's Engagement Crosswalk maps overlapping evidence across frameworks so applicable documentation can be reused rather than collected repeatedly.

A-LIGN has completed more than 36,000 audits for over 6,400 clients worldwide and is also a top-3 Federal Risk and Authorization Management Program [FedRAMP] and HITRUST assessor.3 For IT audit leaders, that combination of SOC 2 scale, multi-framework coverage, and evidence management supports a more coordinated long-term compliance program while preserving the scope, testing requirements, and deliverables that each framework still requires from organizations.

2. Schellman

Schellman is an established audit and assessment firm serving organizations with complex security assurance requirements across multiple industries. Its capabilities extend beyond SOC 2 to ISO standards, FedRAMP, HITRUST, and various Payment Card Industry [PCI]-related assessments.4

This broad coverage makes Schellman particularly relevant to enterprises operating across commercial and regulated environments. Organizations with numerous customer requirements or formal security obligations may benefit from working with an experienced assessment provider familiar with different reporting expectations and control frameworks.

Its multi-framework experience matters when internal teams coordinate complex security assessments with business operations, technology changes, and stakeholder requests.

When evaluating Schellman, IT audit leaders should carefully examine the proposed engagement scope, auditor qualifications, evidence-management processes, and arrangements for coordinating overlapping assessments across different compliance frameworks.

Schellman's broad assessment expertise makes it a credible option for enterprises with diverse assurance obligations. The appropriate fit depends on organizational complexity, regulatory requirements, and the scope of planned assessments.

3. KPMG

KPMG is a global professional-services organization offering SOC assurance alongside cybersecurity, risk, audit, tax, consulting, and other enterprise services. That broader model makes it relevant to large organizations that want SOC reporting considered within wider governance, risk, and business priorities.

For enterprises with established internal audit functions or complex regulatory environments, KPMG can provide SOC assurance within a broader professional-services relationship. This can suit organizations that already work with the firm across related risk, controls, or transformation initiatives and prefer to coordinate those activities through a familiar provider.

Its SOC engagement should still be evaluated on its own terms. IT audit leaders should confirm the responsible audit entity, team experience, proposed scope, testing approach, and independence requirements before proceeding.

Compared with a dedicated compliance-audit provider, KPMG's distinguishing feature is the breadth of the surrounding professional-services relationship rather than a singular focus on multi-framework compliance audits.

4. BARR Advisory

BARR Advisory is a specialist security compliance and assurance provider offering SOC 2 services alongside ISO and HITRUST-related engagements. Its focused service portfolio makes it relevant to mid-market organizations developing formal assurance programs.

For businesses responding to customer security questionnaires, contractual requirements, or expanding compliance obligations, specialist experience can help clarify the scope and preparation involved in planning and completing independent assessments.

BARR's multi-framework capabilities remain relevant beyond an initial SOC 2 engagement. IT audit leaders can assess how the firm coordinates evidence collection, communicates requirements, and manages assessments as compliance programs develop.

Organizations considering BARR should review the proposed CPA engagement team, audit methodology, available framework coverage, and support for recurring reporting cycles.5

BARR's focused approach makes it a credible option for mid-market businesses developing

structured assurance programs. The appropriate fit depends on organizational readiness, reporting obligations, and the scope of future assessments.

How should IT audit and risk leaders choose between these firms?

The appropriate SOC 2 audit firm depends on existing assurance obligations, future compliance requirements, internal resources, and the preferred provider model.

A-LIGN suits organizations managing SOC 2 alongside ISO 27001, HITRUST, and other frameworks. Its single-provider model and A-SCEND's evidence-reuse capabilities support coordinated assessments by reducing repeated evidence collection across compliance cycles.

Schellman serves enterprises requiring broad commercial and regulatory assessment coverage. Its multi-framework expertise supports organizations managing complex security assurance programs and diverse stakeholder requirements.

KPMG suits large enterprises integrating SOC assurance with broader governance, audit, and risk-management priorities. Its professional-services model supports these needs within established enterprise audit relationships.

BARR Advisory serves mid-market organizations prioritizing specialist SOC 2 and related compliance assessments. Its focused expertise supports businesses developing and maintaining formal security assurance programs.

Before selecting a provider, organizations should compare audit scope, credentials, evidence management, future compliance needs, and total costs, including internal resources.

Aligning SOC 2 audits with long-term compliance goals

Selecting an SOC 2 audit partner requires considering more than the next reporting deadline. Independent assurance credibility, internal workloads, and future compliance requirements all affect long-term suitability as organizational security priorities continue to evolve over time.

As organizations adopt additional frameworks, coordinated assessment planning and evidence reuse can become increasingly valuable. The right fit is a provider whose capabilities support both current reporting obligations and the organization's evolving assurance strategy.

- 1SOC 2: compliance
- 2ISO/IEC 27001 information security management systems
- 3Understanding baselines and impact levels in FedRAMP
- 4PCI data security standard (PCI DSS)
- 5System and Organization Controls: SOC suite of services

Summary

The right SOC 2 audit firm depends on existing assurance obligations, future compliance requirements, internal resources and the preferred provider model. A-LIGN suits organizations that manage SOC 2 alongside ISO 27001, HITRUST and other frameworks. Schellman serves enterprises that need broad commercial and regulatory assessment coverage. KPMG suits large enterprises that integrate SOC assurance with broader governance, audit and risk-management priorities. BARR Advisory serves mid-market organizations that prioritize specialist SOC 2 and related compliance assessments. Before you select a provider, compare audit scope, credentials, evidence management, future compliance needs and total costs, including internal resources, and confirm the responsible audit entity for the SOC engagement.