Global SOC 2 Benchmarking 2026

Analysis of 82 SOC 2 report records across 12 contributing countries.

Why This Benchmark Matters

01 See where you stand

Compare your SOC 2 scope and approach with what we see across the benchmark.

02 See what may need attention

Identify whether areas as logical access, change management or third-party responsibilities need more attention. For new SOC 2 journeys: conduct a readiness assessment before the first report.

03 Decide what to improve

Focus improvements on the areas that matter most for your clients and risk profile.

Type 2 is the predominant reporting model

SOC 2 is widely used by technology, SaaS and fintech companies to provide customers with independent assurance over areas such as security, logical access and change management.

For organizations without a SOC 2 report, increasing customer expectations may be a reason to consider whether SOC 2 is becoming relevant.

For organizations that already have SOC 2, this benchmark helps show how their approach compares with the market and where improvements may be useful.

SOC 2 is becoming a market expectation for technology companies

About the benchmark: 82 SOC 2 report records were assessed across 12 contributing countries. Data availability varies by metric, so findings based on smaller samples should be treated as directional. Automation information was available for 18 of the 82 reports.

Type 2 is the predominant reporting model	Broader coverage is common	The number of controls differs considerably	An unqualified opinion does not mean no issues were found	Automation remains an opportunity
75 of 82 reports, or 91.5%, were Type 2 reports. The remaining 7 reports, or 8.5%, were Type 1 reports.	More than 80% of reports included at least one additional Trust Services Criterion beyond Security. This means that many reports also cover areas such as Availability or Confidentiality.	The reports contained between 45 and 236 TSC controls, with a median of 100. The middle 50% contained between 76 and 118 controls. The right number of controls depends on the organization's scope and risk profile. More controls do not automatically mean better assurance.	73 of 82 reports, or 89.0%, had an unqualified opinion. However, 42 of those 73 reports, or 57.5%, still contained one or more exceptions.	Automation information was available for 18 of 82 reports. Across those reports, 472 of 1,584 controls, or 29.8%, were identified as automated. This indicates opportunities to reduce manual effort in control execution, evidence collection and monitoring.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

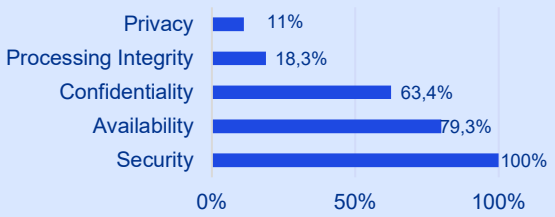
What the Benchmark Reveals

A peer reference for assessing how your SOC 2 approach compares with market practice.

SOC 2 reports can differ considerably in scope, number of controls, exceptions and third-party responsibilities. This benchmark helps organizations see how their SOC 2 approach compares with market practice and where a more focused, risk-based approach may be useful.

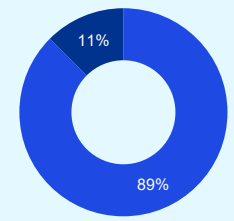
TSC & Control Distribution

Security is included in all SOC 2 reports, while additional criteria should be selected based on the organization's services, customer commitments and risks.



Control Performance & Outcomes

Opinion, %



■ Unqualified ■ Qualified

42 of the 73 unqualified reports, or 57.5%, contained one or more exceptions. An unqualified opinion should therefore not be interpreted as an exception-free report. Among the nine qualified reports, recurring themes were seen in areas such as governance and oversight, logical access and risk management. Given the small number of qualified reports, these themes should be viewed as directional.

The benchmark helps organizations see where their SOC 2 approach is broadly in line with market practice and where greater focus may be needed.

Third Party & Shared Responsibility

64 reports included CUECs, with a median of 6.5. These are controls that customers are expected to operate. 52 reports included CSOCs, with a median of 7. These are controls expected from relevant third-party service providers.

Customer and Subservice Responsibilities
Organizations should understand which controls they perform themselves and which depend on customers or third parties.

Delivery & Scalability

29.8%

Share of controls identified as automated
472 of 1,584 controls across the 18 reports with available automation information.

What this means
Automation and AI can help reduce manual effort in areas such as evidence collection, control monitoring and exception analysis.

AI is a forward-looking consideration and was not separately measured in the benchmark.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

From Benchmark Insights to Action

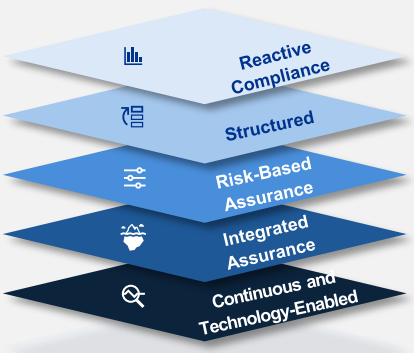
The benchmark is not a maturity score or a target that every organization should copy. It provides a reference point to help organizations make better decisions about scope, controls, responsibilities and automation based on their own risk profile.

Key Takeaways & Common Pitfalls

KPMG perspective: areas to focus on	Common challenges	Practical response
01 Choose the right scope More than 80% of reports included criteria beyond Security. This does not mean every organization needs the same coverage. The scope should reflect the services provided, customer commitments and relevant risks.	⚠ **Security-only scope** *Scope falls short of customer commitments.*	**Map TSCs to customer commitments**
02 Focus on the controls that matter The reports contained between 45 and 236 controls. Rather than targeting a specific number, organizations should focus on controls covering their most important risks, such as logical access, change management and third-party dependencies..	⚠ **Control inflation** *Overly granular controls drive effort and exceptions.*	**Rationalize controls to key risks**
03 Make responsibilities clear CUECs were included in 64 reports and CSOCs in 52 reports. Organizations should clearly understand and document which controls depend on customers or third-party service providers.	⚠ **Unmanaged carve-outs** *Dependencies listed but not monitored.*	**Monitor CSOCs & SOC reports**
04 Look beyond the opinion 42 of the 73 unqualified reports still contained exceptions. Organizations should therefore look at recurring issues and remediation, not only whether the final opinion was qualified or unqualified.	⚠ **Recurring exceptions** *Same areas fail without root-cause fix.*	**Fix root causes, not instances**
05 Use automation and AI where they add value Automation information was available for 18 of 82 reports, with 472 of 1,584 controls, or 29.8%, identified as automated. Automation and AI can help reduce manual effort in areas such as evidence collection, control monitoring and exception analysis, while maintaining appropriate human review.	⚠ **Manual routine controls** *Manual, repeatable controls and evidence processes may create unnecessary assurance effort.*	**Prioritize rule-based controls, evidence generation and repeatable assurance workflows for automation.**

KPMG SOC 2 maturity perspective

Illustrative progression from reactive compliance toward more integrated and continuous assurance.



- *Periodic and largely reactive audit preparation, with controls and evidence collection still mostly manual.*
- *Defined control ownership, documented processes, and repeatable assurance activities.*
- *Controls are prioritized based on the organization's services, risks and customer commitments.*
- *One control framework, based on the organization's risk profile, supports SOC 2 and other relevant assurance requirements.*
- *Automation and AI support monitoring, evidence collection and exception analysis, with human oversight.*

The appropriate target depends on the organization's risk profile, customer expectations, size and complexity. The progression serves as an illustration only and does not assess maturity across the broader market.



Rob van der Gaarden
Director
E: vanderGaarden.Rob@kpmg.nl



Martina Ghisalberti
Senior Manager
E: Ghisalberti.Martina@kpmg.nl



Justin Bleh
Assistant Manager
E: jbleh@kpmg.com

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



kpmg.com/socialmedia

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Public