2024 SOC BENCHMARK REPORT:

Preparing for the Challenges of 2025

Evaluate Your System & Organization Controls (SOC) Program and That of Your Service Providers Against Industry Standards

Contents

INTRODUCTION

Gain Key Insights into SOC Reporting, Compliance and Evolving Control Challenges to Strengthen Your Risk Mitigation Efforts

We are pleased to present the 2024 CBIZ and CBIZ CPAs P.C. SOC Benchmark Study, an annual report offering unique insights into third-party risk management (TPRM), which you can use to assess your SOC program or that of your service providers. This year, we've expanded the study, analyzing 193 SOC reports — up from 154 in the previous year — and introducing new categories, including the average number of Complementary User Entity Controls (CUEC) and Complementary Subservice Organization Controls (CSOC). Additionally, we've included year-over-year comparisons to track key market trends.

Key Takeaways: Comparing 2023 to 2024

Although the 2024 results were similar to 2023 in many ways, there were some notable differences. Below is a year-over-year comparison.

Confidentiality on the Rise

This year, the number of SOC 2 reports that include confidentiality as an in-scope category increased significantly, from 34% in 2023 to 64% in 2024. This indicates a growing focus on protecting sensitive information across service providers.

Working Smarter with SOC 2+

We observed an increase in SOC 2+ reports, incorporating multiple security frameworks into a single report, rising to 9.6% of all reports. This reflects service providers' improved ability to leverage internal controls across multiple security frameworks, such as ISO and HIPAA, streamlining their compliance efforts.

New Control Failures Related to IPE

For the first time, we noted control failures specifically related to Information Provided by Entity (IPE). This comes after years of scrutiny around the completeness and accuracy of audit evidence populations, marking a new area of focus for control failures.

Issuance Periods Still Have Outliers

While no reports were issued over 300 days after the audit period (as was the case in 2023), 15% of reports still took more than 100 days to be finalized. This shows improvement, but outliers remain, emphasizing the need for timely audit processes.

Exceptions Don't Always Lead to Qualified Opinions

Despite some reports containing a high number of control exceptions (8-10), many did not result in qualified opinions. This underscores the importance of thoroughly understanding the reasons behind exceptions and ensuring alignment with the audit opinion conclusion.

SOC Reporting: A Benchmarking Guide

Organizations regularly benchmark their Sarbanes-Oxley (SOX) compliance frameworks against industry peers and should adopt a similar approach for third-party compliance by assessing SOC reports. As the $85 billion outsourcing industry continues to expand, with increasing reliance on third-party providers for critical operations and sensitive data management, evaluating the risks associated with these providers is more important than ever.

The CBIZ and CBIZ CPAs P.C. 2024 SOC benchmark study offers valuable insights, enabling service providers to enhance the efficiency and effectiveness of their SOC reports, ultimately improving service delivery.

This report aims to highlight significant trends, opportunities for improvement and best practices in SOC reporting to help service providers optimize their processes, mitigate risks and enhance customer satisfaction.

The Limitations of Security Questionnaires and the Value of SOC 2 Reports

Many organizations continue to rely on security questionnaires to assess vendor IT security, but these tools present significant limitations. Security questionnaires, often lengthy and reliant on self-assessments, allow organizations to provide an idealized picture of their controls. In fact, according to a study by the Cyentia Institute, 84% of companies utilize these questionnaires, with some containing over 2,500 questions. Yet only 34% of TPRM professionals find them useful.

In contrast, SOC 2 reports provide a more reliable demonstration of an organization's preparedness to manage security threats, offering independent assurance.

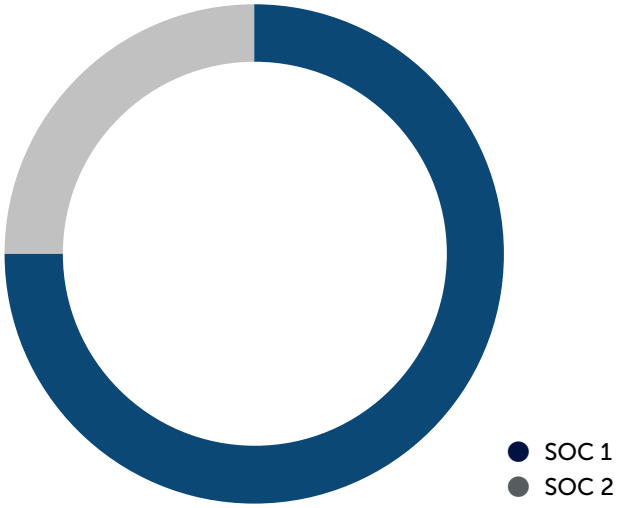
Number of SOC 1 Reports Reviewed

120

Number of SOC 2 Reports Reviewed

73

SOC 1 V. SOC 2 Reports Represented in this Study:



The findings in this report will help you:

- *Assess how your SOC program rates versus those of your peers.*
- *Identify opportunities to enhance your SOC program.*
- *Identify opportunities to streamline your SOC compliance efforts with modern software.*
- *Learn ways to reduce common compliance areas of exception.*

What Type of SOC Report is Required?

Among all service providers, the most common motivation for obtaining a SOC report was a request from a customer or vendor seeking assurance regarding the control structure. Whether a SOC 1 or SOC 2 is required depends on specific parameters.

SOC 1 compliance is required when:

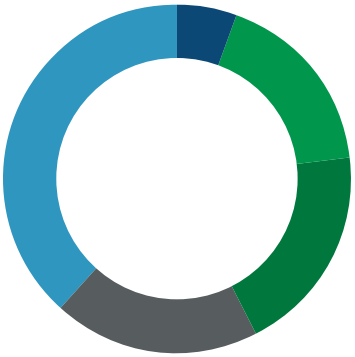
- Your organization provides professional services that may impact financial reporting for your customers.
- Any customers are public entities.

SOC 2 compliance is required when:

- Security is a top concern for your customers and/or vendors.
- Your organization is seeking opportunities for upselling to larger customers (who will likely require SOC 2 compliance).

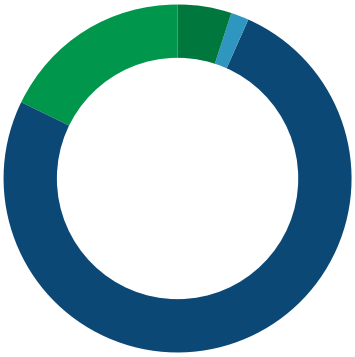
We evaluated 193 SOC 1 and SOC 2 reports from service providers spanning industries and of different sizes and makeups.

Service Provider Overview



Under 100MM	38.3%
100MM-<1B	19.2%
1B-<10B	19.2%
10B<100B	17.6%
100B+	5.7%

Period of Coverage



3-11.75 Months	17.6%
12 Months	75.6%
13-22 Months	1.6%
N/A (Type 1)	5.2%

Location

West	27.5%
Midwest	15.5%
Northeast	36.3%
South	20.7%

Number of Employees

1-99	17.6%
100-999	27.5%
1,000 - 9,999	20.2%
10,000 - 99,999	24.9%
100,000+	9.8%

Industry

Asset Management	5
B2B Services	8
Banking	4
Consulting	5
Crypto	3
Data Analytics	1
Energy	4
Engineering	1
Financial Services	30
Gambling	1
Government	4
Healthcare	4
Hosting / Data Centers	13
Human Capital Services	32
Insurance	11
IT Service Provider	14
Marketing	6
Printing	2
Real Estate	2
SaaS	41
Telecommunications	2

Total

193

KEY FINDINGS

The following pages highlight our key findings and their relevance, provide suggestions and best practices for service providers and report users to support SOC compliance.

Key Finding One:

Objective Counts Remain Broad

In 2024, the range of objectives in SOC 1 reports remained broad, ranging from three to 65 (versus two to 56 in 2023). This year, over half of the reports (52.5%) contained one to nine control objectives, consistent with 2023 (53%). A small percentage (3.3%) of reports included more than 20 objectives, raising the overall average from 10 to nearly 12.

One observation we highlight is questioning reports with too few categories (four or fewer). Any SOC 1 report intended to address financial controls should, at a minimum, include IT general controls objectives over security, change management and operations. This alone would account for a minimum of three objectives and would not even consider the relevant financial controls that should be the focus of SOC 1.

Key Takeaways:

- The number of objectives among SOC 1 reports varies greatly.
- It's up to service providers to confirm with their service auditor that the objectives identified are sufficient to provide a comprehensive end-to-end understanding of the control environment.
- If the count appears high compared to the figures in this report, service providers should explore opportunities to reduce and/or consolidate objectives.
- If an objective count seems low, it is the report user's responsibility to confirm it covers all areas of control pertinent to their business.

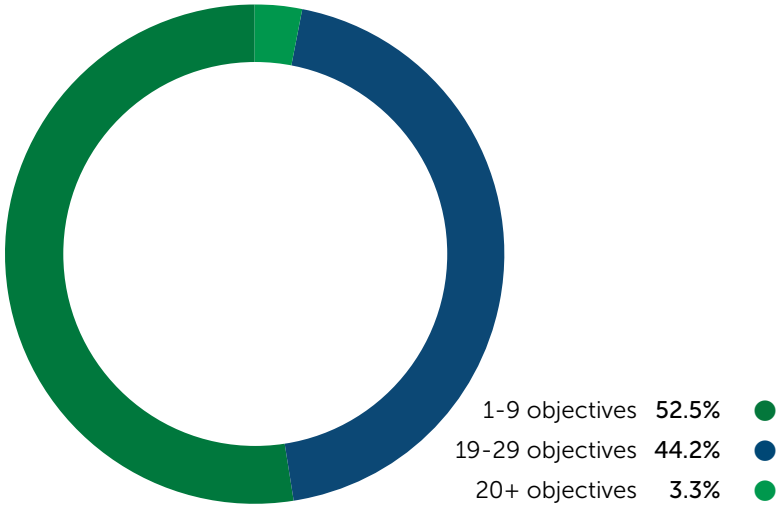
Range in Number of Objectives

3 - 65

Average Number of Objectives

11.9

Number of Objectives



Number of Categories (SOC 2):

Security Remains Key as Confidentiality Gains Importance

Our analysis of SOC 2 reports nearly doubled to 73 in 2024 from 38 in 2023, offering a more comprehensive view. Consistent with 2023, 100% of the SOC 2 reports included security as an in-scope category, despite an AICPA FAQ from November 2020 stating it's not required. Given the importance of security controls, it's hard to imagine a scenario where security wouldn't be relevant.

Confidentiality saw a significant increase, rising from 34% to 64.4%, driven by the relatively small number of controls required for compliance, its focus on protecting sensitive data and its relative ease to achieve versus privacy.

We were excited by the notable increase in organizations adopting a one-to-many testing approach across security frameworks. Specifically, we saw 9.6% of SOC 2 reports be issued as SOC 2+, meaning that reports included criteria for not only SOC 2 but also another security framework, such as HIPAA.

Key Takeaways:

- Availability continues to be the second most common category, slightly increasing from 71% to 75% of analyzed reports.
- The two additional criteria required for achieving confidentiality, compared to the 18 criteria for privacy, continue to be a significant deterrent for organizations considering the inclusion of privacy.
- It's important for organizations pursuing SOC 2+ with added security frameworks to be aware that some security standards are highly protective of their proprietary frameworks and may not permit the issuance of a combined report. It is best to consult with a service auditor prior to considering pursuit.

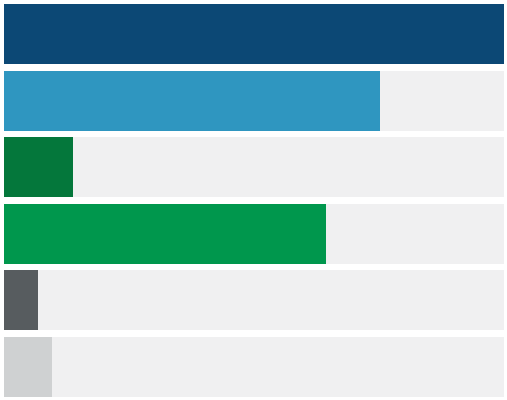
Security Only SOC 2 Reports

12

Multi-Criteria SOC 2 Reports

61

Criteria Most Commonly Included in SOC 2 Reports



Security:	100%
Availability:	75.3%
Processing Integrity:	13.7%
Confidentiality:	64.4%
Privacy:	6.8%
SOC 2+:	9.6%

Number of Controls (SOC 1):

Consistency in SOC 1 Controls Reflects Stability

The number of SOC 1 controls remained consistent year over year, with an average of 69.95 this year compared to 68 last year. While there's a joke about auditors sticking to past practices — "Why did the auditor cross the road? Because the workpapers said that is what was done last year" — there's some truth to it. Audit firms invest time in ensuring the scope is accurate, so the minimal change in controls is a reassuring sign of consistency and stability.

Key Takeaways:

- The number of reports with 18-50 controls this year was nearly flat from last year (46.7% in 2024 vs. 46% in 2023).
- Surprisingly, the number of SOC 1 reports with over 200 controls increased (albeit by a small margin) from 1% last year to 3% this year. This may be likely due to added scope for some larger institutions to continue to expand coverage of their SOC 1 in support of customers' SOX requirements.

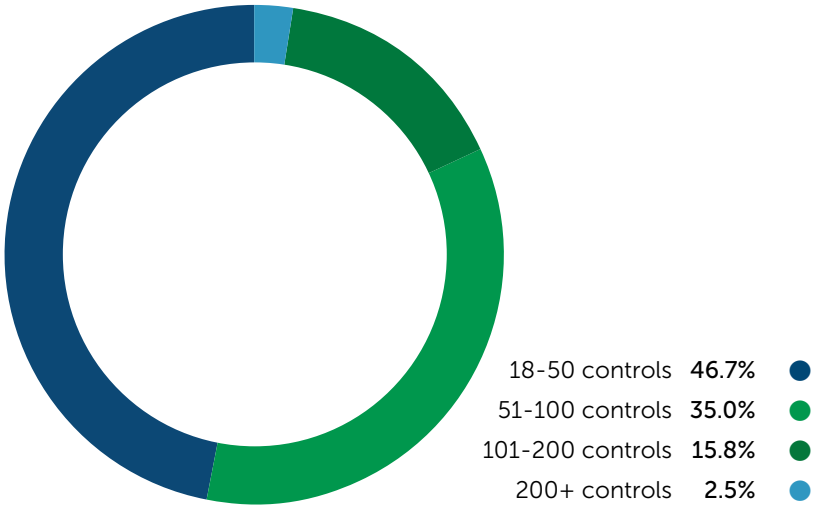
Range in Number of Controls

18 - 431

Average Number of Controls

70

Control Ranges in SOC 1 Reports



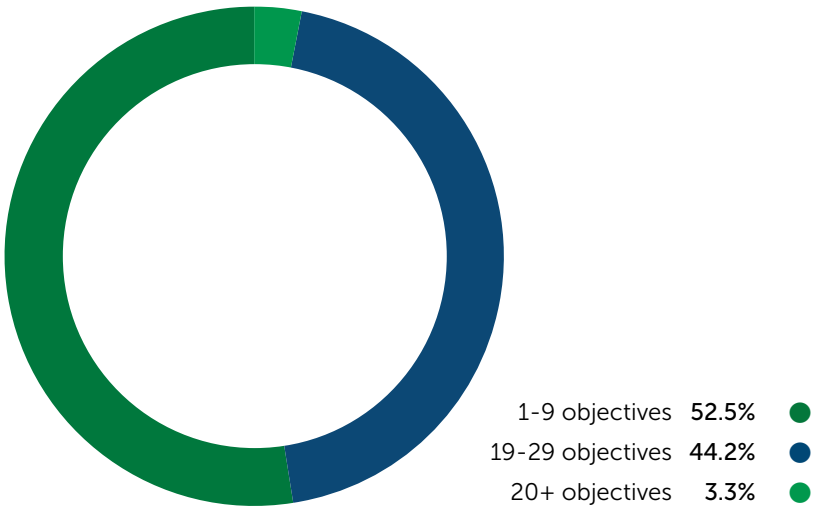
Range in Number of Objectives

3 - 65

Average Number of Controls

11.9

Number of Controls



Number of Controls (SOC 2):

Efficient SOC 2 Reporting Requires Clear Mapping and Balanced Control Coverage

We urge our fellow audit firms to provide more concise mappings of "unique" controls tested in SOC 2 reports. While some firms offer clear listings of unique controls and their mappings to SOC 2 criteria, this isn't always true. We did our best to account for controls in the reports analyzed, but it was sometimes difficult to decipher without unique identifiers. Unconcise unique labeling also makes it harder for readers to decipher the effort input into a firm's SOC 2 (e.g., 100 controls is a much more rigorous effort than, say, 50). It should be valuable information shared with readers.

Last year, we separated our analysis into total controls and security-specific controls. Reports with 150 or more security controls increased, possibly due to redundant controls across categories or auditors reviewing more controls. Most clients can achieve sufficient security coverage with 50-60 controls, and adding more may lead to unnecessary costs and effort. A SOC 2 report should balance control redundancy and efficient compliance.

Key Takeaways:

- In a few reports, we continued to see some service auditors that mapped SOC 2 controls to every single point of focus within individual criteria despite clear AICPA guidance on the fact that there is no need to do so.
- There was a leap in the number of SOC 2 with >150 security controls from 16% last year to 23% this year. Considerations as to the drivers would be speculation without all the audit facts. However, we see a higher number of controls in reports driven via software companies assisting in audits that utilize more general "checklists" for suggestions of possible controls. This lack of a true controls rationalization of solely what is necessary (versus a check-the-box exercise) tends to inflate the number of controls.

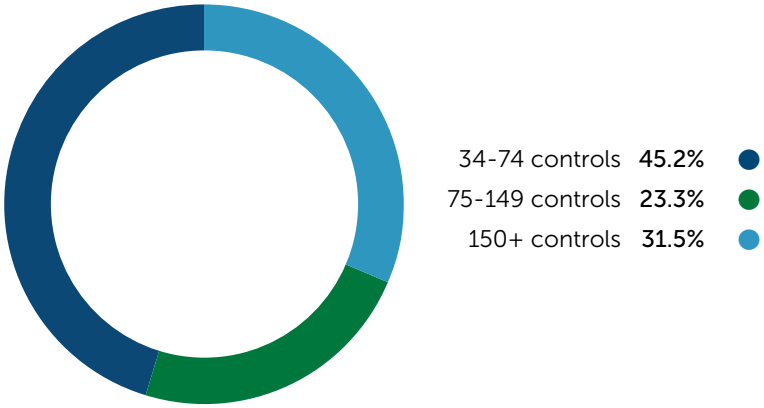
Range in Number of Controls

34 - 382

Average Number of Controls

124.4

Control Ranges in SOC 2 Reports



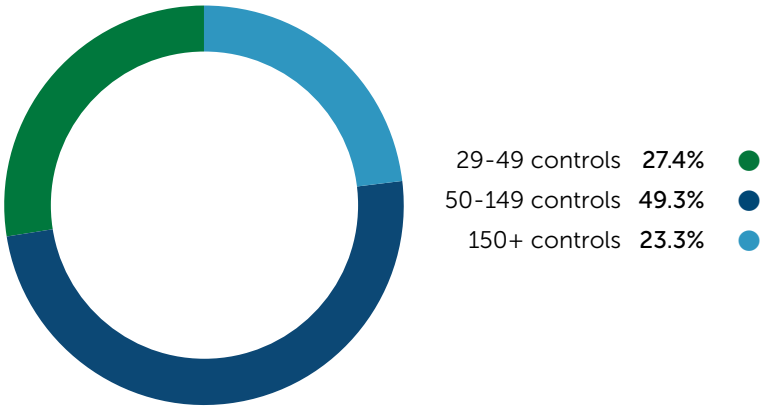
Range in Number of Security Objectives

29 - 375

Range in Number of Security Objectives

107.2

Security Control Ranges in SOC 2 Reports



Subservice Providers:

Increased Transparency on Subservice Providers Reflects Growing Dependency

There was little change in the subservice model used by service providers, with most continuing to rely on the carve-out model, excluding subservice providers from the audit scope. This makes sense, as it's unrealistic to expect major providers, like Amazon, to participate in every client's SOC audit.

However, we were pleased to see a slight increase in reports, including subservice providers, rising from 82% last year to 89.6% this year. This reflects the reality that most service environments depend on multiple providers. A Gartner study from October 2022 showed that 78% of companies use 16 or more tools to manage their environments, with some managing over 46 tools, often involving more than 10 vendor relationships.

Key Takeaways:

- The 4% of reports that utilized a combination of inclusive and carve-out subservice models were all instances of parent-child relationships among the two organizations. This makes sense as these two organizations would be more open (and incentivized) to collaboration on a single SOC report.
- Reminders from the prior year:
  - » Service providers should have a comprehensive list of subservice providers. Although not required, we suggest disclosing that list to report users so they may fully assess their risk.
  - » If that information is not provided, the report user may want to inquire about the report's scope and question why subservice providers were not mentioned by name.

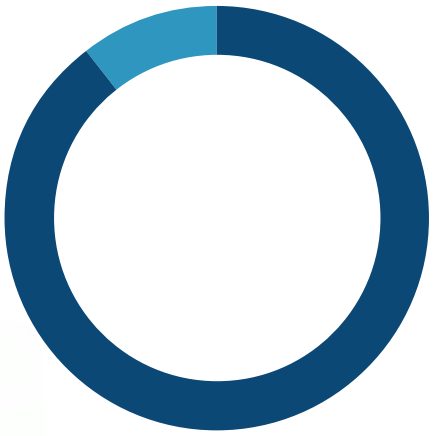
Range in Subservice Providers Used

0 - 14

Average Number Used

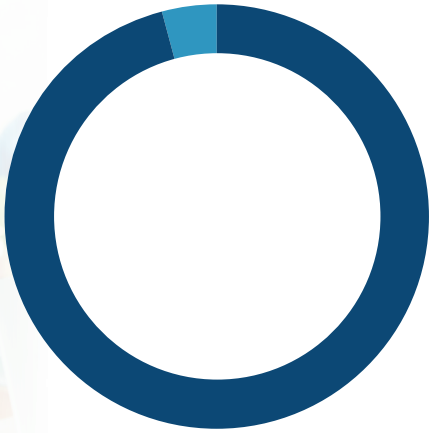
2.8

Subservice Provider Utilization Rates



Used	89.6%
Did Not Use	10.4%

Subservice Provider Utilization Rates



Carve-out	96.0%
Combination	4.0%
Inclusive	0.0%

Internal Audit

Internal Audit Utilization Declines, But Its Value Shouldn't Be Overlooked

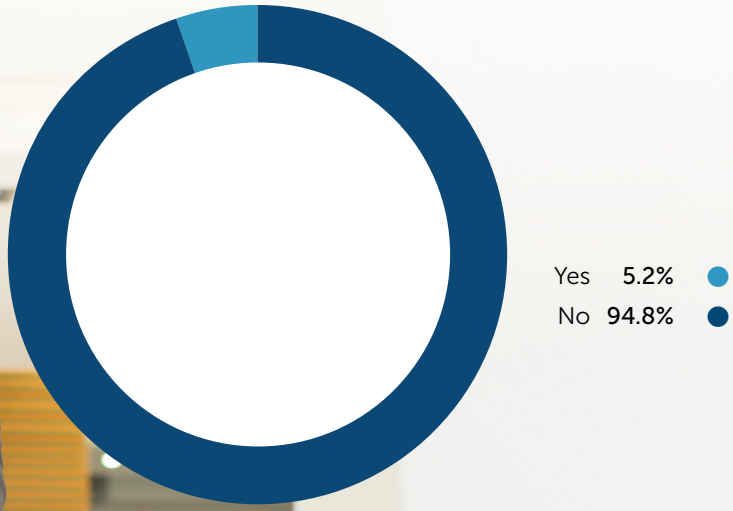
Last year, we noted that only 8% of SOC reports utilized internal audit (IA) to reduce testing, and this year, that number has decreased further to 5.2%. This decline may be due to the October 2022 AICPA SOC 2 guide, which no longer requires service auditors to disclose reliance on IA work, as the auditors absorb the associated risk.

While we understand this change, we encourage service providers to continue pushing their auditors to rely on IA, as it could help reduce the audit scope and potentially lower fees.

Key Assumptions:

- Usage of IA by the service auditor often comes down to a few factors:
  - The existence of an internal audit function. (Many smaller organizations that do not have internal audits are still able to achieve SOC compliance.)
  - Expertise and availability of internal audit to support the SOC audit.
  - The service auditor's reliance model. Some audit firms have stringent reperformance standards for internal audit work, so the benefits of reliance may be minimal or not worth the time or investment.

Internal Audit Utilized?



Control Exceptions

Monitor Control Exceptions as Data Accuracy Gains Focus

The percentage of SOC reports with exceptions slightly increased from 51% last year to 54.9% this year, while the average number of exceptions per report decreased from 2.7% to 1.73%. The top four reasons for exceptions remain consistent:

- Business approvals/reviews (16.5% in 2024; 18% in 2023)
- User access reviews (15.6% in 2024; 15% in 2023)
- Terminations (12% in 2024; 13% in 2023)
- Change management (11.7% in 2024; 14% in 2023)

One notable change, though, was that exceptions related to information provided by entity (IPE) appeared for the first time this year. This reflects a growing focus on the completeness and accuracy of data in SOX programs. Therefore, it is no surprise to see a "trickle-down" effect of IPE exceptions starting to be more prominently called out in SOC reports.

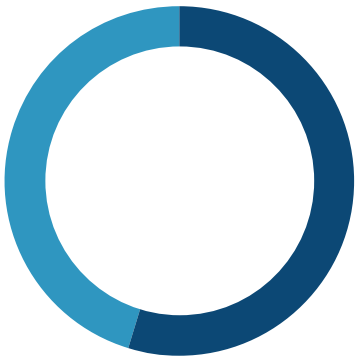
Range In Number Of Exceptions

1 - 16

Average Number Of Exceptions

1.7

Exceptions Included?

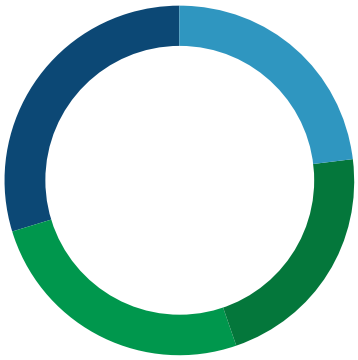


Yes 54.9%
No 45.1%

Additional Common Types Of Exceptions

Financial Review, Code of Conduct/ Policy not reviewed, Background Checks, Performance Evaluations, Access Review not performed (Physical/Logical), Environmental Controls, New Hires, 3P Reviews, Confidentiality, Transfers, Passwords, Administrative Access, Physical Access, Back-Ups, Risk Assessment, Network Controls

Most Common Types Of Exceptions



Business Aprovals/Reviews 17.4%
User Access Reviews 15.1%
Terminations 12.8%
Change Management 13.7%

Key Takeaways:

Reminders from the prior year:

- Service providers and report users alike should understand the full scope of exceptions and best practices for control improvements.
- High numbers of exceptions should warrant a conversation to ensure the issue is remediated and to confirm a service provider's overall commitment to managing its control environment.

Recommendations for areas of high control exceptions:

- Change management: Utilization of a centralized repository for documenting and tracking changes is essential. If your ticketing system can be configured to make certain fields mandatory (e.g., testing approval, approval for promotion, etc.), this is even better as it ensures that key control points cannot be overlooked.

User access reviews: Exceptions here often fall into one of a few categories:

- Non-performance: The simplest issue warrants the simplest recommendation. Set reminders to perform the activity on its required cadence.
- Lack of documentation: Similar to change management, utilizing a centralized repository such as an IT help desk or ticketing system ensures that all information is available upon request.
- Segregation of duties: In some cases, reviewers were called out for reviewing their own access. This can be easily rectified by adding a second reviewer in instances where this may occur.
- IPE: Auditors have started to get used to maintaining evidence of completeness and accuracy of populations, but this hasn't always been the case for control owners. Control owners should maintain the parameters or query how they generate any listing of users they are reviewing to support the completeness/accuracy of the reports they have reviewed.

Audit Opinion

Numerous Exceptions Without Qualification Warrant Further Inquiry

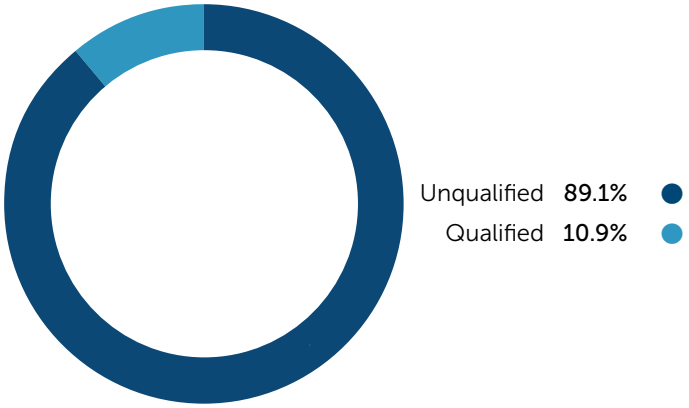
The percentage of SOC reports with qualifications saw a slight increase from 8% last year to 10.9% this year, shifting the primary reason for qualifications from business approvals/reviews to user access reviews (UAR). We're pleased to report that environmental controls, which accounted for 14% of qualifications in the prior year, fell completely off the radar this year with zero instances. This was an exceptionally surprising area for qualification last year, especially when a handful of the qualifications due to environment controls were related to the SOC 1 report. We are still scratching our heads a year later, trying to understand how environmental controls may have impacted financial reporting and been necessary for being in scope for SOC 1.

On a side note, while auditors must explain the rationale for qualifications, there's no requirement to document why reports aren't qualified, even when exceptions are numerous. Acknowledging that reports may not contain all of the background and facts in instances of many exceptions (8-10, most of which were in the same criteria or objectives), we would love to see a push for greater transparency on conclusions. If users of service providers do observe reports with high numbers of exceptions and an unqualified opinion, we encourage these readers to ask prudent questions about the reasons for exceptions and how the organization is addressing them. This year, we noticed two to three reports where many exceptions seemed to revolve around related objectives (SOC 1) or criteria (SOC 2), e.g., user provisioning. However, the report still was positioned as unqualified.

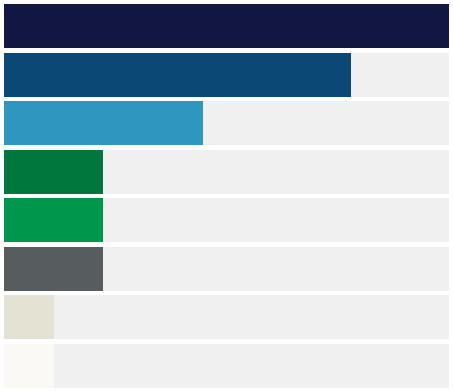
Key Takeaways:

- The next buckets of most common reasons for qualification (all at 7.1%) included lack of performance of background checks, code of conduct or employee handbooks not reviewed by personnel upon hire and inappropriate administrative access.
- Background checks and code of conduct/employee handbooks typically fall within human resources' responsibility and should be monitored for adherence. While SOC 2 is heavily focused on IT controls, organizations should not lose sight of the importance of entity-level controls.

Qualified v. Unqualified Opinion



Most Common Types of Exceptions



User Access	32.1%
Business Approvals/Review	25.0%
Change Management	14.3%
Background Checks	7.1%
Code of Conduct/ Policy Not Reviewed	7.1%
Admins	7.1%
Performance Evals	3.6%
Backups	3.6%

Emphasis of Matter

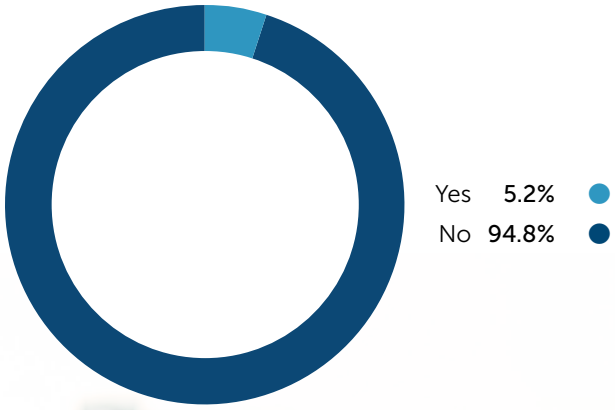
Reduced Emphasis of Matter Highlights Need for Greater Clarity in Control Assessments

Emphasis of matter (EOM) paragraphs, as a reminder, are included at the auditor's discretion. They are intended to call the report user's attention to areas of significance outside the key audit matters section. This information is included when the auditor deems it fundamental to a user's understanding of the report.

There was no significant change in EOM usage from last year to this year, but we anticipate a potential decline next year. While EOM highlights key details for readers, recent AICPA updates to the SOC guides may reduce its use. It was a subtle change that was not highlighted as a key change but one that readers of SOC reports should be aware of.

Previously, if most controls under a certain criterion didn't need to operate (for example, no security incidents or breaches occurred), additional language was required in the auditor's report to signify that the auditor was unable to test the effectiveness of such controls. It highlighted that the service auditor's opinion provided more limited assurance in those areas. Auditors are no longer required to modify their opinion on control effectiveness in such cases. This shift may now prompt report readers to seek greater clarity on when controls were tested and when opinions were based solely on design assessments. In cases of limited testing, users should consider contacting service providers to understand better how critical areas, like incident management, are managed for their own added assurance.

Emphasis of Matter Paragraph Included?



Description of the System

Striking the Right Balance in System Descriptions: Detailed but Focused

The system description comprehensively overviews an organization's systems, processes and controls. It aims to tell auditors and service users the who, what, when, why and how key controls operate. The description should sufficiently cover all key controls tested within the report and enhance a reader's understanding of "specifically" how risks are managed. Vague descriptors such as, "A process is in place for the organization to document, test and approve of system changes," tell a reader little about critical control points to provide reasonable assurance sufficient controls are in place. Conversely, an overly detailed explanation may provide unnecessary details and "bury" the essence of what readers should focus on. This balance in mind led to our interest in how the lengths of system descriptions may vary across SOC 1 and SOC 2 reports.

This year, we found that the average number of pages in Section 3 (system description) increased slightly over last year, indicating that service providers are offering more detailed insights into their systems and control environments, which is a positive trend. The greatest range of descriptions varied from 10-19 pages (43.5%) to 20-49 pages (42.5%). This, again, largely emulated that of the prior year (at 40% for both ranges).

Key Takeaways:

- While there is no ideal length for a system description, we advise service providers to avoid extremes — either too short (5-9 pages, which 6.7% of reports fall into) or too long (50+ pages, 7.3% of reports). Short descriptions may leave out key control details, while overly lengthy descriptions risk overwhelming the reader and diluting focus on critical information. A balanced and clear system description is the key to effective understanding.
- The number of reports with a description of only five to nine pages (thankfully) decreased from 15% last year to 6.7% this year. We challenge service organizations that fall into this category because if the system description intends to provide details on processes on all key controls (50-60 for a SOC 2), then it seems not much insight has been provided.

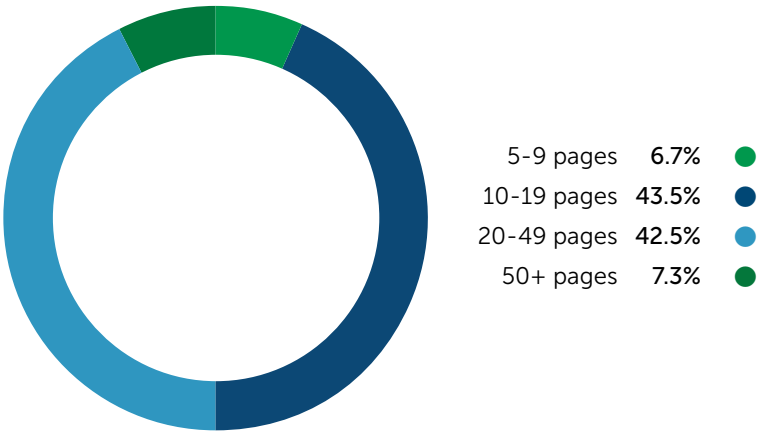
Range In Number of Pages

7 - 88

Average Number of Pages

24.4

System Description Length Ranges



Duration to Issue

Timely Issuance of SOC Reports Reflects Process Efficiency, and Delays Require Scrutiny

The issuance period refers to the time between the end of the audit period and the issuance of the final SOC report and is one of our favorite areas for review. For public companies, timely report release is crucial, yet many readers overlook this aspect, which can offer indirect insights into the audit process and more specifically, process efficiency.

Our analysis for this year shows that 85% of reports are issued within 100 days, with many mid to large-sized audit firms aiming for 45-60 days. Delays beyond this are typically due to either the service organization not providing information on time or conflicts on the auditor's end. If the issuance period is extended, it's worth inquiring with the service provider to understand the cause, especially if internal priorities may have delayed compliance efforts (possibly signifying insufficient attention on key control focus).

Key Takeaways:

- Last year, we reviewed one SOC report issued 535 days after its period end. Thankfully, the longest reporting period this year was only 215 days (7+ months) after period end. This is an improvement, but still an area where we would desire more information as system users.
- The number of reports issued 100-299 days after period end also decreased from 21% last year to 15% this year.

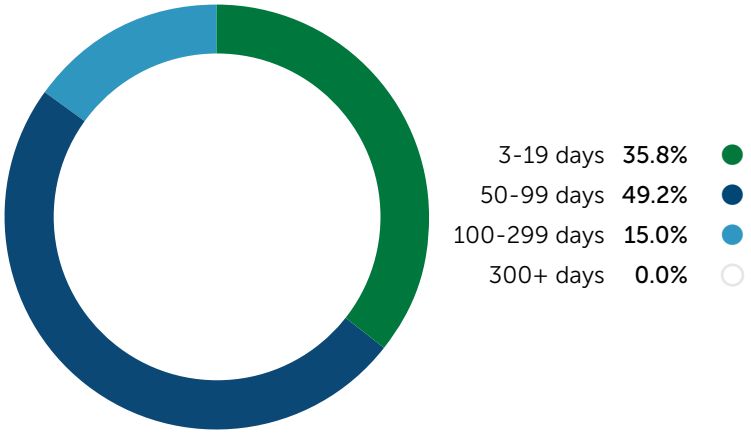
Range in Days Taken to Issue a Report

2 - 215

Average Number of Days

69.9

Duration to Issue Ranges



Complementary User Entity Controls

A Critical Component for Ensuring Comprehensive Control Coverage

Complementary User Entity Controls (CUECs) are controls that service organizations expect their customers to implement to ensure the effectiveness of the overall control environment. These controls are essential because they guide users on what areas to focus on rather than leaving them to guess.

Most reports we analyzed contained 0-20 CUECs across both SOC 1 and SOC 2 (81.9%). This "average" varied slightly amongst SOC 1 (75.8%) and SOC 2 (91.8%). Those reports with CUEC of greater than 20 CUECs saw SOC 1 with 24.2% and SOC 2 with 8.2%.

Key Takeaways:

- A higher number of CUECs for SOC 1 is likely attributable to financial auditors relying upon SOC 1 in support of their SOX audits. This means that these reports receive a higher degree of scrutiny on the completeness/accuracy of CUEC listings, and auditors are likely to make service organizations aware if they feel there may be any missing controls.
- SOC 2 reviews, on the other hand, are often limited to IT personnel in evaluating key service providers and are often more focused on overall opinion (qualified/unqualified) and/or what exceptions may exist.
- While the AICPA's SOC 2 guide suggests that CUECs may not always be required, it's difficult to imagine a modern service environment where users have no responsibility for control management. Users should investigate if a report lacks CUECs, especially given today's reliance on cloud providers and technology partners. A careful review of CUECs is important when analyzing SOC 2 reports.

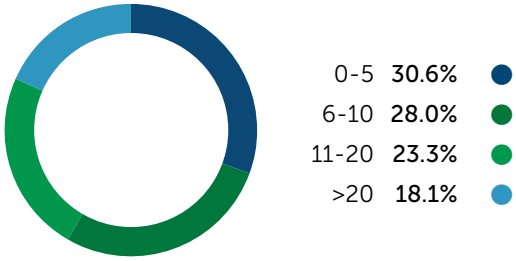
Range In CUECs – SOC 1 or SOC 2

0 - 79

Average In CUECs – SOC 1 or SOC 2

12.5

Complementary User Entity Controls (CUECs)



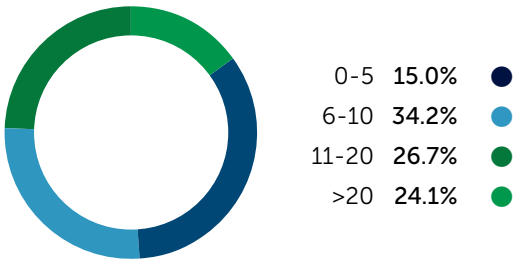
Range In CUECs – SOC 1 Only

0 - 79

Average In CUECs – SOC 1 only

14.7

Complementary User Entity Controls (CUECs)



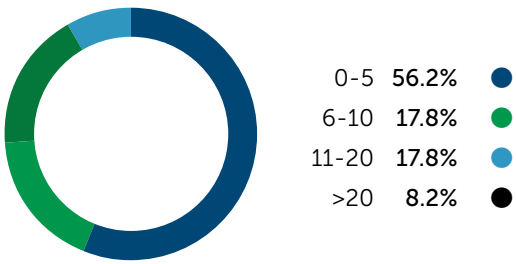
Range In CUECs – SOC 2 Only

0 - 73

Average In CUECs – SOC 2 only

8.9

Complementary User Entity Controls (CUECs)



Complementary Subservice Organization Controls

Ensuring Subservice Provider Controls Support Service Commitments

Complementary Subservice Organization Controls (CSOCs) are controls that service organizations expect their subservice providers to implement, working alongside the service organization's own controls to ensure service commitments and system requirements are met. According to the AICPA, service auditors can suggest improvements for CSOC disclosures, but the final decision rests with the service organization's management. This means that service organizations need to consider the controls their users rely upon due to outsourcing certain functions to provide their readers with a comprehensive listing of CSOC.

In our inaugural analysis of CSOC, we noted that, on average, service organizations had roughly 10 CSOC controls, with most having between 0 and 5. In the SOC 1 reports we reviewed, 85% had 20 or fewer CSOC controls. SOC 2, however, saw 91.8% reports with 20 or fewer controls.

Key Takeaways:

- We recommend focusing on outliers, especially if no CSOCs are identified, as this could signal gaps in the overall control framework.

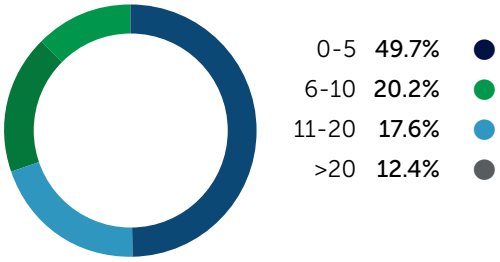
Range in CSOCs – SOC 1 or SOC 2

0 - 90

Average in CSOCs – SOC 1 or SOC 2

10.1

Complementary Subservice Organization Controls (CSOCs)



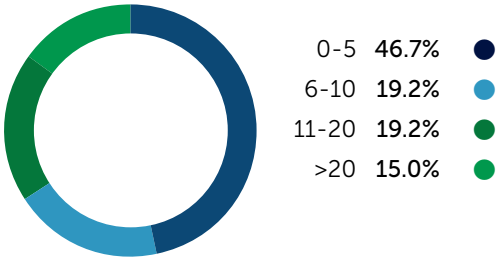
Range in CSOCs – SOC 1 Only

0 - 90

Average in CSOCs – SOC 1 Only

10.8

Complementary Subservice Organization Controls (CSOCs)



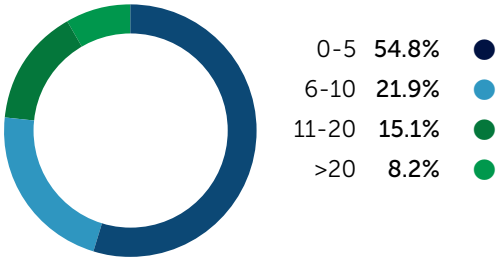
Range in CSOCs – SOC 2 Only

0 - 88

Average in CSOCs – SOC 2 Only

9.1

Complementary Subservice Organization Controls (CSOCs)



Conclusion

Navigating the Future of SOC Compliance: Tailored Strategies for Evolving Risks

Refine Your Approach, Mitigate Risks and Stay Ahead in Third-Party Oversight with Key Insights from the 2024 SOC Benchmarking Study

The 2024 SOC Benchmarking Study highlights the ongoing need for a well-structured and transparent SOC compliance framework. As cybersecurity threats grow and reliance on third-party providers increases, organizations must continuously refine their SOC processes. This report offers valuable insights to help organizations benchmark their efforts, streamline compliance and minimize risks effectively.

SOC compliance has become a critical part of assessing third-party risk, and the findings in this study underscore the importance of tailoring SOC reports to each organization's unique needs. No two control environments are the same, and there is no one-size-fits-all solution. Engaging with knowledgeable service auditors and fostering open dialogue can help organizations balance their compliance efforts, avoiding unnecessary burdens or vulnerabilities.

As you progress, we encourage you to assess how your SOC report compares to industry peers, focus on areas outside group averages and address key questions with your service auditor. Outliers provide opportunities to either streamline or enhance your SOC framework. Have proactive conversations with your service auditor or service provider and inquire about instances where your report may deviate. Doing so can optimize your SOC compliance strategy and ensure your organization is well-positioned to manage third-party risks and regulatory demands.

For More Information Contact:

Scott Woznicki | 617.761.0673 | scott.woznicki@cbiz.com

Scott Woznicki is a CBIZ CPAs P.C. Shareholder and the National System and Organization Controls (SOC) Practice Director. A Certified Public Accountant and Certified Information Systems Auditor, he has more than 20 years of experience providing global consulting, accounting, advisory and attest services to privately held and public companies. In addition to providing System and Organization Controls (SOC) examinations (SOC 1, SOC 2, etc.) and agreed-upon procedures, Scott has extensive experience in operational reviews, risk assessments, internal and IT audits, Sarbanes-Oxley (SOX) and cybersecurity.

Learn more at CBIZ.COM

CBIZ

Learn more at CBIZ.COM

CBIZ is a consulting, tax and financial services provider that works closely with CBIZ CPAs P.C., an independent CPA firm that provides audit, review and other attest services. In certain jurisdictions, CBIZ CPAs P.C. operates under its previous name, Mayer Hoffman McCann P.C.